UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

SECURITIES AND EXCHANGE COMMISSION, Plaintiff, v. SOLARWINDS CORP. and TIMOTHY G. BROWN, Defendants.	)	Civil Action No. 23-cv-9518-PAE Jury Trial Demanded

AMENDED COMPLAINT

Plaintiff Securities and Exchange Commission ("SEC"), for its Amended Complaint against Defendants SolarWinds Corp. ("SolarWinds" or "the Company") and Timothy G. Brown ("Brown") (collectively, "Defendants"), alleges as follows:

SUMMARY

1. From at least October 2018 through at least January 12, 2021 (the "Relevant Period"), Defendants SolarWinds and its then-Vice President of Security and Architecture, Brown, defrauded SolarWinds' investors and customers through misstatements, omissions, and schemes that concealed both the Company's poor cybersecurity practices and its heightened—and increasing—cybersecurity risks. SolarWinds' public statements about its cybersecurity practices and risks painted a starkly different picture from internal discussions and assessments about the Company's cybersecurity policy violations, vulnerabilities, and cyberattacks. Illustratively, in October 2018, the same month that SolarWinds conducted its Initial Public Offering, or IPO, through a registration statement with only generic and hypothetical cybersecurity risk disclosures, Brown wrote in an internal presentation that SolarWinds'

"***current state of security leaves us in a very vulnerable state for our critical assets***."[1] This was not a one-off comment: it had been Brown's assessment of the state of SolarWinds' cybersecurity for more than a year leading up to the Initial Public Offering.

2. This is not a case about isolated failures, attempts at compliance that were good but less than perfect, or the SEC seeking to impose its own set of specific cybersecurity protocols on SolarWinds or all public companies. As the alleged facts show, SolarWinds and Brown recognized and documented the Company's long-standing, pervasive, systemic, and material cybersecurity deficiencies. Indeed, an April 15, 2020 email to Brown warned that "***we have a systemic issue around lack of awareness for Security/Compliance requirements with most if not all [of the information technology group's] projects.***" Nevertheless, SolarWinds and Brown made public statements that directly contradicted the internal assessments and omitted the risks those deficiencies posed. SolarWinds and Brown misled the investing public by concealing the materially increased risks of a cyberattack that SolarWinds faced because it systemically failed to follow many of the industry-standard cybersecurity practices to which the Company claimed to adhere.

3. The true state of SolarWinds' cybersecurity practices, controls, and risks ultimately came to light only following a massive cyberattack—***which exploited some of SolarWinds' poor cybersecurity practices***—and which impacted thousands of SolarWinds' customers. That attack, termed SUNBURST, compromised SolarWinds' Orion software platform, a flagship product that the Company considered to be a "crown jewel" asset and which accounted for 45% of its revenue in the first nine months of 2020.

[1] All emphasis in quotations in this Complaint is added unless otherwise noted.

4. SolarWinds is a publicly traded company that, during the Relevant Period, provided software that thousands of companies and many government agencies used to manage their information technology infrastructure by, for example, monitoring activity on networked servers.

5. When Brown joined SolarWinds in July 2017, he realized that the Company's cybersecurity posture was poor. He also realized that SolarWinds lacked public security policies it could use to assuage customers' concerns about cybersecurity, and that this lack of policies was costing the Company business. So, working with others at SolarWinds, he began a scheme and course of business to mislead the public about the quality of the Company's cybersecurity practices by posting a "Security Statement" and making other public statements that claimed SolarWinds was following good cybersecurity practices, even though Brown and others at SolarWinds knew this was false.

6. SolarWinds and/or Brown made materially false and misleading statements and omissions related to SolarWinds' cybersecurity risks and practices in at least three types of public disclosures:

a) Statements that purported to describe the Company's cybersecurity practices and policies, including a "Security Statement" posted to the Company's website throughout the Relevant Period;

b) Form S-1 and S-8 Registration Statements and periodic reports filed with the SEC throughout the Relevant Period; and

c) A Form 8-K filed with the SEC on December 14, 2020 regarding the massive SUNBURST cybersecurity incident that impacted SolarWinds' Orion software platform.

7. The Security Statement was materially misleading because it touted the Company's supposedly strong cybersecurity practices. For example, that statement asserted that SolarWinds safely created its software products in a "secure development lifecycle [that] follows standard security practices including vulnerability testing, regression testing, penetration testing, and

product security assessments." It also claimed that SolarWinds servers were "monitored for the detection and prevention of various network security threats." And the Security Statement claimed that SolarWinds' "password policy covers all applicable information systems, applications, and databases [and we] enforce the use of complex passwords." Additionally, it stated that SolarWinds had "[a]ccess controls to sensitive data in our databases, systems, and environments [that] are set on a need-to know / least privilege necessary basis." All those statements were materially false and misleading.

8. The misleading Security Statement concealed from the public the Company's known poor cybersecurity practices throughout the Relevant Period. These poor cybersecurity practices included SolarWinds' (a) longstanding failure to consistently maintain a Secure Development Lifecycle (or "SDL") to securely develop the software it developed and provided to thousands of customers, (b) unresolved failure to adequately monitor its networks, (c) repeated failure to enforce the use of strong passwords on all systems, and (d) persistent, years-long failure to remedy access control problems.

9. SolarWinds' SEC filings similarly concealed the Company's poor cybersecurity practices. They contained general, high-level risk disclosures that lumped cyberattacks in a laundry-list of risks alongside "natural disasters, fire, power loss, telecommunication failures…[and] employee or contractor theft or misuse." The cybersecurity risk disclosure was generic and hypothetical, allowing for negative consequences "[i]f we sustain system failures, cyberattacks against our systems or against our products, or other data security incidents or breaches." This disclosure failed to address known risks. For example, it warned of an inability to defend against unanticipated techniques but failed to disclose that SolarWinds had determined that it was not taking adequate steps to protect against anticipated and known risks, including

failing to follow the Secure Development Lifecycle and other practices outlined in the Security Statement. These general warnings were then repeated verbatim in each relevant filing, despite both the ongoing failures to meet their own Security Statement and the increasing red flags in 2020 that SolarWinds was not only being specifically targeted for a cyberattack, but that the attackers had already gotten in.

10. In and around the same time that SolarWinds was making these materially misleading public statements, Brown and other SolarWinds employees knew that SolarWinds had serious cybersecurity deficiencies. Internal emails, messages, and documents from the same period described many known material cybersecurity risks, control issues, and vulnerabilities. These internal statements dramatically contradicted SolarWinds' public disclosures relating to its cybersecurity practices, risks, controls, and vulnerabilities. And they showed many of the same problems persisting unresolved for years, as the examples below highlight:

SolarWinds Failed to Maintain A Secure Development Lifecycle for Years

a. A January 2018 email to senior managers bluntly admitted that the Security Statement's Secure Development Lifecycle section was false, and described a "simple" scheme by which, rather than amend the Security Statement to make it accurate, SolarWinds would conceal the present falsity of the representations and work to make them true eventually: "I've gotten feedback that ***we don't do*** some of the things that are indicated in the [Security Statement's SDL section]. I want to make sure that you all have an answer to this. The simple response is: There is improvement needed to be able to meet the security expectations of a Secure Development Lifecycle. We will be working with teams throughout 2018 to ***begin incorporating*** the SDL into their development lifecycle."

b. By 2020, portions of SolarWinds' flagship Orion software platform were still not developed under an SDL process, and SolarWinds employees warned Brown and others that this was a problem. In June 2020 an employee asked: "Do we have SDL process enforced for Orion Improvement Program ["OIP"] server? ***If SDL is not enforced for OIP, we should do it ASAP*** and consider additional actions to make sure that OIP is very well protected." As the employee surmised, the OIP was not in fact covered by the SDL as of June 2020.

SolarWinds Had Poor Access Controls for Years

c. A June 2017 presentation shared with the CIO described an "***unnecessary level of risk***" from too many accounts having expanded administrator-level access, including the "[s]ystem team" using administrator accounts during routine operations.

d. In June 2018, SolarWinds Network Engineer D[2] identified a "security gap" relating to SolarWinds' remote access virtual private network, which allowed access from devices not managed by SolarWinds. Network Engineer D warned that this setup was "***not very secure***" and later explained that someone exploiting the security gap "can basically do whatever without us detecting it until it's too late" which could lead to a "***major reputation and financial loss***" for SolarWinds.

e. An August 2019 presentation that Brown prepared warned that "[***a]ccess and privilege to critical systems / data is inappropriate.***"

f. Presentations that Brown helped prepare in March and October 2020 highlighted "[***s]ignificant deficiencies***" in SolarWinds' access controls.

[2] Persons and entities not charged in this Amended Complaint, but referred to repeatedly, are identified by pseudonyms. All pseudonyms that are used in both this Amended Complaint and the original Complaint refer to the same persons / entities.

SolarWinds Recognized It Faced Increasingly Worrisome Attacks in 2020

g. In a July 2020 presentation, Brown warned about threat actors' familiarity with a critical SolarWinds software platform, noting that the threat actors "***[k]now how to deploy software, shut off backup, etc.***"

h. In a July 2020 email to Brown, a member of the Engineering team described being "spooked" by Orion's activity during a cyberattack on a U.S. Government Agency A server. Brown agreed that the incident was "***very concerning***" and continued, "As you guys know ***our backends are not that resilient*** and we should definitely make them better." Brown also determined that there were only two possibilities: that the attacker was already present on the agency's system, or that someone was trying to use Orion in a larger attack.

i. In October 2020, Cybersecurity Firm B also notified SolarWinds personnel about a cyberattack involving Orion. InfoSec Employee F then informed Brown: "[Cybersecurity Firm B] in touch with customer support and it seems they had a breach similar to [U.S. Government Agency A]." The specific similarities between the attacks that SolarWinds employees recognized and flagged for Brown at the time made clear that, of the two possible scenarios Brown outlined after the attack on U.S. Government Agency A, it was now likely that a threat actor was using Orion as part of a larger attack against multiple SolarWinds customers.

SolarWinds Had More Cybersecurity Problems Than It Could Fix

j. SolarWinds' CIO identified undersized staff to respond to cybersecurity incidents as a "key risk" in 2019.

k. A September 2020 Risk Acceptance Form flagged for Brown and others "the risk of legacy issues in the Orion Platform" and warned "[t]he volume of security issues being identified over the last month have ***outstripped the capacity*** of Engineering teams to resolve."

l. In November 2020, a SolarWinds Information Security employee sent an instant message to Senior InfoSec Manager E with a link to a list of vulnerabilities in the Orion platform stating, "***The products are riddled and obviously have been for many years***." That same month, a SolarWinds' network engineer complained: "We filed more vulnerabilities then [sic] we fixed. And by fixed, it often means just a temporary fix…but the problem is still there and it's huge. I have no idea what we can do about it. Even if we started to hire like crazy, which we will most likely not, it will still take years. ***Can't really figure out how to unf**k this situation.*** Not good."

11. Even though Brown and/or other SolarWinds employees and executives knew about these longstanding risks, vulnerabilities, and attacks, SolarWinds' cybersecurity risk disclosures did not disclose them in any way, either individually or by disclosing the increased and increasing risk they collectively posed to SolarWinds. In sum, the total mix of information that SolarWinds disclosed to the investing public was materially misleading because it concealed SolarWinds' pervasive cybersecurity problems and increased risks.

12. To be clear, SolarWinds' poor controls, Defendants' false and misleading statements and omissions, and the other misconduct described in this Amended Complaint, would have violated the federal securities laws even if SolarWinds had not experienced a major, targeted cybersecurity attack. But those violations became painfully clear when SolarWinds experienced precisely such an attack.

13. Between January 2019 and December 2020, SolarWinds experienced one of the worst cybersecurity incidents in history, the SUNBURST "'supply chain' cyberattack," which exploited some of the cybersecurity failings described above and compromised SolarWinds' "crown jewel" Orion product.

14. As early as June 2018, SolarWinds information technology employees knew the Company had a cybersecurity weakness or security gap that allowed access to the Company's virtual private network ("VPN") through unmanaged devices such as cell phones and laptops that were neither owned nor operated by the Company. In January 2019, threat actors accessed SolarWinds' systems through the VPN using an unmanaged device and a local system administrator account. The actors then had broad, undetected access to SolarWinds' systems. (It is possible that the threat actors first accessed SolarWinds' systems at an earlier time and through other means, but the earliest confirmed access was in January 2019 through the VPN security gap that had been identified in June 2018.)

15. Using their access, the threat actors inserted malicious code into three software builds for SolarWinds' Orion products. SolarWinds then delivered these compromised products to more than 18,000 customers across the globe. The malicious code provided the threat actors with the ability to access the systems of these compromised customers, provided certain other conditions were met, and became known as the SUNBURST attack.

16. During 2020, Brown learned about increasing cybersecurity attacks against, and vulnerabilities involving, Orion and other SolarWinds products. This included cybersecurity attacks against two customers who were using the Orion product, U.S. Government Agency A in May 2020 and Cybersecurity Firm B in October 2020.

17. Shortly after the October 2020 attack against Cybersecurity Firm B, SolarWinds employees including Brown recognized similarities between that attack and the attack on U.S. Government Agency A. But when personnel at Cybersecurity Firm B asked SolarWinds employees if they had previously seen similar activity, InfoSec Employee F falsely told Cybersecurity Firm B that they had not. He then messaged a colleague, "[***W***]***ell I just lied***."

18. In early December 2020, a third customer, Cybersecurity Firm C, discovered that it too had become the victim of a cyberattack through SolarWinds' Orion platform. Cybersecurity Firm C quickly identified the malicious code in SolarWinds' Orion product. On December 12, 2020, Cybersecurity Firm C notified SolarWinds' CEO of the malicious code and shared the relevant code with Brown in a manner that made the malicious code readily apparent to Brown as a cybersecurity professional. Brown immediately recognized that the malicious code identified by Cybersecurity Firm C was the same vulnerability in the Orion platform that had been previously exploited against U.S. Government Agency A and Cybersecurity Firm B.

19. On December 14, 2020, SolarWinds filed a Form 8-K with the SEC disclosing that its Orion network monitoring software contained malicious code that had been inserted by threat actors as part of a supply-chain attack. The Form 8-K was drafted by a group of executives, including Brown, and signed by SolarWinds' CEO. That Form 8-K was materially misleading in several respects, including its failure to disclose that the malicious code at issue had been actively exploited against SolarWinds' customers multiple times over at least a six-month period in the incidents involving U.S. Government Agency A, Cybersecurity Firm B, and Cybersecurity Firm C.

20. On December 14, 2020, the day it filed the Form 8-K first announcing the SUNBURST attack against the Orion platform, SolarWinds' stock price dropped more than 16%.

It dropped at least an additional 8% the next day. The stock price continued to drop and lost approximately 35% of its value by the end of the month as SolarWinds disclosed more details of the SUNBURST attack, and as news outlets reported that internal sources had warned SolarWinds for several years about the Company's cybersecurity risks and vulnerabilities. Investors who purchased SolarWinds stock before this price drop suffered pecuniary harm.

DEFENDANTS

21. **SolarWinds** is a Delaware corporation with its headquarters in Austin, Texas. Founded in 1999, SolarWinds conducted its first IPO in 2009 and remained a public company until February 2016, when it was acquired by several private equity firms in a take-private transaction. The Company conducted a second IPO in October 2018 and has remained a public company since.

22. **Timothy G. Brown**, age 59, is a resident of Salado, Texas. Brown was responsible for the overall security program at SolarWinds throughout the Relevant Period. Between July 2017 and December 2020, Brown was an officer of SolarWinds, serving as its Vice President of Security and Architecture, and head of the Information Security group at SolarWinds (referred to at SolarWinds and in this Amended Complaint as "InfoSec"). Since January 2021, he has been SolarWinds' Chief Information Security Officer, a position that did not exist at SolarWinds before the SUNBURST attack was discovered. In his role as Vice President of Security and Architecture, Brown was responsible for the Company's ongoing security efforts, as well as security architecture within its products. Brown also signed sub-certifications attesting to the adequacy of SolarWinds' cybersecurity internal controls, which SolarWinds' executives relied on in connection with SolarWinds' periodic reports that were filed with the SEC. Throughout the

Relevant Period, Brown also served as SolarWinds' cybersecurity spokesperson, making many public statements about SolarWinds' cybersecurity practices.

OTHER RELEVANT PERSONS AND ENTITIES

23. U.S. Government Agency A is a federal agency that was a SolarWinds customer during the Relevant Period.

24. Cybersecurity Firm B is a cybersecurity firm that was a SolarWinds customer during the Relevant Period.

25. Cybersecurity Firm C is a cybersecurity firm that was a SolarWinds customer during the Relevant Period.

26. Network Engineer D is a former SolarWinds employee.

27. Senior InfoSec Manager E is a SolarWinds employee who was one of two SolarWinds employees who reported directly to Brown during the Relevant Period.

28. InfoSec Employee F is a SolarWinds employee who, at all relevant times, reported directly to Senior InfoSec Manager E and indirectly to Brown.

29. Customer G is a multinational information technology company.

30. Engineering Manager H is a SolarWinds employee who, during the Relevant Period, reported to the Company's Chief Technology Officer.

31. Investing Entity I is a large pension fund that acquired a significant number of SolarWinds shares during the Relevant Period.[3]

32. Analyst J is a securities analyst who followed, and wrote investment reports regarding, SolarWinds and other technology companies during the Relevant Period.

[3] The actual name of Investing Entity I and the companies at which Analysts J & K work have been previously disclosed to the Court. Additionally, the true names of all pseudonymous persons and entities have been provided to counsel for the Defendants in Rule 26 Disclosures and therefore they should not be treated as anonymous.

33. Analyst K is a securities analyst who followed, and wrote investment reports regarding, SolarWinds and other technology companies during the Relevant Period.

34. Security & Compliance Manager L is a Security & Compliance Senior Program Manager who was one of two SolarWinds employees who reported directly to Brown during the Relevant Period. Security & Compliance Manager L worked in this position from approximately February 2019 through at least the end of the Relevant Period, and provided general support for the security team regarding policies, processes, and procedures. Prior to February 2019, she worked in a different role for SolarWinds on a contract basis.

35. SolarWinds Chief Executive Officer, Chief Financial Officer, Chief Technology Officer, and Chief Information Officer at the relevant times are referred to as the "CEO," "CFO," "CTO," and "CIO," respectively.

JURISDICTION AND VENUE

36. The SEC brings this action, and this Court has subject matter jurisdiction over this action, pursuant to Sections 20 and 22 of the Securities Act of 1933 [15 U.S.C. §§ 77t and 77v] (the "Securities Act"), Sections 21 and 27 of the Securities Exchange Act of 1934 (the "Exchange Act") [15 U.S.C. §§ 78u and 78aa, and 28 U.S.C. § 1331].

37. Defendants SolarWinds and Brown, directly or indirectly, singly or in concert with others, made use of the means or instruments of transportation and communication in interstate commerce, or of the mails, or of the facilities of a national securities exchange in connection with the acts, transactions, and practices alleged in this Amended Complaint.

38. Throughout the Relevant Period, SolarWinds was engaged in the offer and/or sale of securities. This included its October 2018 IPO, which was registered with the SEC through a Form S-1 registration statement that became effective on October 18, 2018 and an additional

public offering of shares through a Form S-1 registration statement filed on May 20, 2019. The Company also registered additional offerings in April 2019, December 2019, and February 2020 on Forms S-8 for shares offered pursuant to the Company's Employee Stock Purchase Plan ("ESPP"). Multiple employees, including employees not participating in the fraud, purchased stock through the ESPP throughout 2019 and 2020, and the Company received money from those purchases. Each Form S-8 incorporated by reference the Company's most recent annual report on Form 10-K, as well as all periodic reports filed between the date of the most recent annual report and the Form S-8.

39. During the Relevant Period, Brown was engaged in the offer and/or sale of securities and received money or property by selling SolarWinds stock at prices inflated, at least in part, by the misconduct described in this Amended Complaint. Specifically, Brown exercised options and sold SolarWinds stock during 2020, receiving more than $170,000 in gross proceeds when SolarWinds' stock price was inflated by the misstatements, omissions, and schemes discussed in this Amended Complaint. This included the sales listed in the chart below, each of which was processed through the New York Stock Exchange:

Sale Date	**Shares Sold**	**Price**	**Gross Proceeds**
2/10/2020	1500	$18.92	$28.384.24
2/27/2020	1000	$17.65	$17,646.10
5/6/2020	1000	$17.22	$17,220.00
5/22/2020	500	$17.95	$8,973.80
8/13/2020	2500	$19.54	$48,849.00
8/18/2020	1500	$19.90	$29,842.71
8/31/2020	1000	$21.21	$21,205.00
Total	**9000**		**$172,120.85**

40. Venue lies in this District pursuant to Securities Act Section 22(a) [15 U.S.C. § 77v(a)] and Exchange Act Section 27(a) [15 U.S.C. § 78aa] because, among other things, some of the acts, practices, transactions, and courses of business alleged in this Amended Complaint

occurred within the Southern District of New York and were effected, directly or indirectly, by making use of means or instrumentalities of transportation or communication in interstate commerce, or the mails, or the facilities of a national securities exchange. For example, beginning with the Company's October 2018 IPO, and continuing through the present, the Company's stock was publicly traded using the ticker symbol "SWI" on the New York Stock Exchange, located in this District. The four lead investment firms that managed the Company's IPO are all either based in this District or maintain large offices in this District. An October 18, 2018 press release by SolarWinds directed persons interested in obtaining a copy of the prospectus for its IPO to contact one of those four firms and provided contact addresses. Three of those addresses were in this District, and the fourth was in the Eastern District of New York. In addition, individuals residing in the Southern District of New York purchased and sold SolarWinds stock during the Relevant Period.

41. Additionally, throughout the Relevant Period, two private investment companies collectively owned more than 70% of SolarWinds' common stock. Each of those companies has business locations in this District.

42. In September and October 2023, SolarWinds and Brown each executed tolling agreements that tolled two weeks of conduct for the purposes of the statute of limitations.

FACTS

A. SolarWinds Designs and Sells Software That Other Companies and Government Agencies Use to Manage Their Computer Networks.

43. Both now and during the Relevant Period, SolarWinds designs and sells network monitoring software used by many businesses, as well as state, federal, and foreign governments to manage their computer systems. Among other things, SolarWinds' products provide information technology professionals with visibility into network utilization and equip

information technology departments to detect, diagnose, and resolve network performance issues. SolarWinds also sells its own cybersecurity products. During the Relevant Period, SolarWinds had more than 300,000 customers, including 499 of the companies making up the Fortune 500.

44. Orion is an information technology infrastructure and management platform consisting of a suite of products used by customers to manage network system configurations. Orion was SolarWinds' flagship product during the Relevant Period and accounted for 45% of the Company's revenue in the first nine months of 2020. Internally, SolarWinds considered Orion to be one of its "crown jewels," a term used to describe assets that, if compromised, could have a material impact on the Company.

B. Brown and Other SolarWinds Employees Recognized SolarWinds' Poor Cybersecurity Practices, but Then Concealed the Problems to Obtain and Retain Business.

1. Brown Determined that SolarWinds' Poor Cybersecurity Hindered Its Ability to Obtain and Retain Business.

45. Brown joined SolarWinds in July 2017. By August 2017, he had determined that SolarWinds had poor overall cybersecurity. An August 2017 presentation at the monthly SolarWinds Information Technology leadership meeting included a section titled "Security State of the Union" that appears to have been delivered by Brown based on both its content and the fact that the beginning of that section prominently featured a picture of Brown. That presentation pre-dated the posting of the Security Statement on SolarWinds' website. Roughly a month into his tenure at SolarWinds, Brown already recognized that SolarWinds had poor cybersecurity practices, including a lack of employee training on cybersecurity. Brown flagged that the "[c]urrent state of security leaves us in a very vulnerable state for our critical assets. A compromise in these assets would damage our reputation and financially [sic]." The presentation

also acknowledged that SolarWinds needed to "reduce the number of security incidents by implementing industry standard best practices."

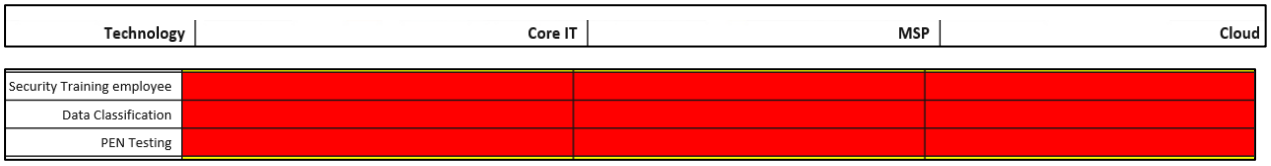
46. Brown and the Company understood that SolarWinds' compliance with cybersecurity best practices was material to SolarWinds' ability to obtain and retain business, and that because of its poor cybersecurity practices, SolarWinds was at risk of losing business.

47. Many SolarWinds customers required their software vendors, including SolarWinds, to answer detailed security questionnaires before purchasing new products or renewing contracts on existing products. The "Security State of the Union" section warned that "Appropriate security policies, procedures, training, PEN testing are required by our commercial customers and asked for in qualifying questionnaires. Without appropriate answers we will lose business." The presentation highlighted that SolarWinds had already lost one recent renewal because it used "free code scanning tools that did not find all vulnerabilities."

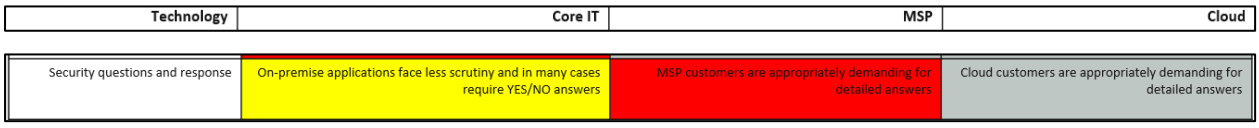
48. Brown emailed a similar presentation—which he described as the "[c]urrent state of security and proposed move to a proactive security model"—to other employees on September 7, 2017. In that presentation, Brown again warned that the "[c]urrent state of security leaves us in a very vulnerable state for our critical assets. A compromise in these assets would damage our reputation and financially [sic]." Brown also repeated many of the same specific warnings about lack of training and other problems from the August 2017 presentation.

49. The September 2017 presentation also included multiple slides appearing to assess various cybersecurity measures across SolarWinds' three business segments (Core IT, MSP, and Cloud) using bright green, yellow, or red filled boxes. Brown admitted in his testimony that the red boxes were for items that needed "more work" or referred to a practice that was "not yet

deployed." Among the areas that were color-coded in red were "Security Training employee," "Data Classification" and "P[enetration] testing," as shown in the excerpts below:



50. In the same September 2017 presentation, on the topic of "Security questions and response," CoreIT is color-coded in yellow with the statement "On-premise applications face less scrutiny and in many cases require YES/NO answers." MSP is color-coded in red, and stated, "MSP customers are appropriately demanding for [sic] detailed answers." The topic of "Cloud" is color-coded in gray with the similar comment that "Cloud customers are appropriately demanding for detailed answers," as shown below:



51. The presentation also warns that the "[l]ack of legally approved security questions/answers are costing us time and customers."

52. The CIO not only knew that SolarWinds' cybersecurity problems could cost it customers but also that those cybersecurity problems were material to the Company's valuation for its then-upcoming IPO. Additionally, in what appear to be the CIO's draft performance self-assessments from January and June 2018, she identified "Identity and Access Management" and "Security Standards" as two of the deficiencies that could adversely impact SolarWinds' "IPO ***valuation***." Even though the document admitted that these were such important issues that they could affect SolarWinds' stock price, it also stated that these problems were not planned to be fixed until 2019—after the IPO.

53. Notably, Brown's September 2017 presentation identified deficiencies in the specific areas that Johnson stated could affect SolarWinds' IPO valuation. With respect to "Identity Management" the presentation noted "many gaps" in all three business lines, as well as "inconsistent management" in the CoreIT business line. In a "Risk Mitigation Plan for IT Security Operations" slide of the same presentation, Brown described the need to "Lock down our critical assets that could cause a major event" including the need to "[l]ock down administrative access and improve identity management processes and procedures." Brown also provided a similar assessment regarding "Identity Management" in a December 2017 presentation, stating that there was "No consistent identity plan for users or for administrators" and identifying "[m]any gaps, inconsistent management." In the same presentation, Brown identified "Identity Management" as a "security product portfolio gap" and included "Identity" as an "area of concern" to be remediated. As discussed below, identity management and access control problems persisted throughout the Relevant Period.

54. In his later July 2018 blog post on security, Brown again underscored how cybersecurity can help companies obtain and retain business: "People often think of security as an insurance policy—something you have to have, like locks on your doors, fire and flood insurance, and business insurance. While these are all true, there are opportunities to think of security as a business enabler, something that can help you open additional doors for your business and stand out from your competition."

55. Additionally, Analyst K confirmed that, at least at the point where cybersecurity problems are starting to affect a company's ability to attract and retain business, if not well before, they are material to investors and something that he would have considered important in determining whether to recommend that investors purchase SolarWinds' stock.

2. Brown Created the Security Statement as Part of a Scheme to Provide False Assurances Regarding SolarWinds' Cybersecurity.

56. Rather than first fix SolarWinds' cybersecurity problems, Brown and others decided to post a "Security Statement" to SolarWinds' website, claiming that it followed procedures and adhered to practices that Brown and others knew, and documented internally, that SolarWinds did not follow.

57. One SolarWinds employee who viewed a draft version of the Security Statement in 2017 described it as "aspirational," meaning it described the state of security that SolarWinds hoped to achieve at some point in the future, not the current state of its cybersecurity practices. Nevertheless, Brown and SolarWinds misleadingly posted the Security Statement on the Company's website and affirmatively sent it to customers claiming it described the practices SolarWinds followed at the time. This was part of the scheme to convince the public and actual or potential customers that the Company was following industry-standard cybersecurity practices when—in fact—it did not follow many of them.

58. SolarWinds posted the Security Statement purporting to describe the Company's cybersecurity practices on its public website in late 2017, before the Company's IPO. Brown was primarily responsible for creating and approving the Security Statement before it was posted. In multiple Company documents, Brown was identified as the "owner" or "approver" of the Security Statement. The "Trust Center" section of SolarWinds' website, which contained the Security Statement, prominently featured a picture of Brown, who was head of the relevant InfoSec group. Brown (or others acting at his direction) disseminated the Security Statement, or a link to the Security Statement, to customers seeking more information about SolarWinds' security practices, and he provided a link to the Trust Center in Company-approved blog posts that he authored and that were posted on a SolarWinds' website.

59. The Security Statement purportedly informed the public of SolarWinds' cybersecurity practices. Similarly, SolarWinds' website assured the public that the Company "is committed to taking our customers [sic] security and privacy concerns seriously and makes it a priority," and that the Company's "security strategy covers all aspects of our business."

60. By its terms, the Security Statement applied to SolarWinds' "information system assets," which consisted of "customer and end-user assets as well as corporate assets." The Security Statement specifically incorporated "the procedures and guidelines defined by SolarWinds[']s security policies" and stated that personnel who handled information system assets had to comply with those policies, guidelines, and procedures.

61. The Security Statement was then used as part of SolarWinds' official response to customer questionnaires regarding its cybersecurity practices. In other words, it was the missing document that Brown said in August and September 2017 that SolarWinds needed to obtain and retain customers. SolarWinds' employees, with Brown's knowledge, regularly disseminated the Security Statement, sending customers hyperlinks in emails or other documents that linked directly to the Security Statement on SolarWinds' website and advising that the Security Statement detailed how SolarWinds was mitigating the risk of cyberattacks.

62. Brown knew the Security Statement was false when it was posted. On December 14, 2017, Brown emailed a presentation regarding his 2017 goals and his self-assessment of their status to his supervisor, the CIO. The presentation again includes boxes that are color-coded in green, yellow, and red noting the status of various projects or practices. "Security questions and response" is in a green box, noting in part that "Public security statement now in place." But the presentation also includes red boxes for things like "PEN[etration] testing" where the assessment warned that there was "No PEN[etration] testing of external properties or internal security" and a

separate red box for "Application PEN[etration] strategy" which was "Limited to MSP solutions." A screenshot showing Penetration or "PEN" testing assessment and several others from this presentation is below:

Security Training employee	Very Very Very limited.
Data Classification	Classification policy in place with GDPR but no automation in place
PEN Testing	No PEN testing of external properties or internal security. Needs to be a priority in early 2018
Policies Security, Data Retention, DR	Policies are getting better with GDPR as a driver. Still more to do if we are going to measure ourselves against NIST or complete an ISO Audit. Still missing a number of standard policies.
Operations review Helpdesk, HR, Support	Inconsistent training, policies and security procedures Should be driven by GDPR functions. A number of bad practices and missing policies in place. Clean desk, physical security, background checks, passwords, secure communications

These assessments contradict the specific representation in the Security Statement that SolarWinds' "secure development lifecycle follows standard security practices including vulnerability testing, regression testing, penetration testing, and product security assessments." In other words, Brown knew from its inception that the Security Statement was false.

63. The December 14, 2017 presentation also repeated many warnings from the August and September 2017 presentations, including that the "[c]urrent state of security leaves us in a very vulnerable state for our critical assets. A compromise in these assets would damage our reputation and financially [sic]."

64. As shown above, Brown knew, or was reckless or negligent in not knowing, that the goal of the Security Statement was to present false assurances that SolarWinds followed good cybersecurity practices. This operated as a scheme and course of business that defrauded not only SolarWinds' customers, but also defrauded SolarWinds investors during the Relevant Period by concealing from them the true risks of investing in SolarWinds.

65. Brown was not the only person at SolarWinds who knew, or was reckless or negligent in not knowing, that the Security Statement was false. In January 2018, shortly after the Security Statement was published, SolarWinds managers complained that "we don't do some of the things that are indicated in" it. But rather than take down, or amend the Security

Statement, SolarWinds managers planned to conceal the failure to follow the public Security Statement and instead work to maybe make it true someday.

66. Other evidence also shows that Brown and SolarWinds misled customers regarding the quality of SolarWinds' cybersecurity practices to win contracts. For example, in 2019, Customer G requested information about SolarWinds' internal security testing before moving forward with a "pending deal." Brown said to other SolarWinds employees, "I'm in control of what we share" and that, in his response to Customer G, "I called the [pending issues] that were partially mitigated as mitigated. This should give [Customer G] enough to move forward with the purchase." One of the problems had been designated by the testers as "critical" and had not been fully mitigated. But Brown, apparently based on a SolarWinds employee's opinion that it was a "non-issue," designated it as "mitigated."

67. Although some of this conduct predates SolarWinds' IPO, it is nevertheless relevant to SolarWinds and Brown's intent, knowledge, recklessness, and/or negligence during the Relevant Period regarding the materially false and misleading statements and omissions in the Security Statement, and the scheme to conceal SolarWinds' poor cybersecurity practices from its customers and investors, which continued throughout the Relevant Period.

68. That the Security Statement was materially false and misleading is corroborated by other documents, including those discussed below, which show that SolarWinds was not adhering to various critical aspects of the Security Statement.

69. Securities analysts who followed SolarWinds considered the opinions of customers regarding SolarWinds products in conducting their evaluations and assessments of whether to recommend buying or selling SolarWinds stock. Those analysts also assumed a basic level of cybersecurity diligence and practices by SolarWinds and would have wanted to know if

SolarWinds was not following industry standard practices by, among other things, as alleged in this Amended Complaint: (1) allowing broad use of administrator access and otherwise maintaining poor access controls; (2) failing to conduct security awareness training; and (3) failing to conduct threat modelling. Analysts would have particularly wanted to know about these issues if they persisted across years, and were brought to the attention of senior managers but remained unresolved.

C. SolarWinds and Brown Falsely Promoted SolarWinds' Cybersecurity Practices in Public Statements During the Relevant Period.

70. Throughout the Relevant Period, SolarWinds and Brown made false and misleading public statements touting the quality of the Company's cybersecurity practices.

71. SolarWinds' Security Statement remained publicly posted on its website, virtually unchanged, throughout the Relevant Period and covered areas including secure development lifecycle, network monitoring, password protection, and access controls, among others.

72. SolarWinds' Security Statement contained multiple materially false and misleading statements, assuring the public that SolarWinds followed well-recognized cybersecurity practices when, in reality, the Company's cybersecurity practices fell significantly short of those assurances. The Security Statement also omitted information necessary to make the information included, in light of the circumstances, not misleading. The false statements and omissions in the Security Statement included, among other things, claiming overall compliance with the widely used and internationally recognized National Institute of Standards and Technology Cybersecurity Framework ("NIST Cybersecurity Framework") for evaluating cybersecurity practices; and representing that SolarWinds followed four specific cybersecurity practices: (1) using a secure development lifecycle when creating software for customers; (2) employing

network monitoring, (3) having strong password protection; and (4) maintaining good access controls.

73. The failures described below represent both individual failures so pervasive in critical areas that they represented systemic problems, and programmatic failures across wide swaths of SolarWinds or even the entire Company. Together, the failures, risks, issues, and incidents described in this Amended Complaint so affected SolarWinds' cybersecurity posture that SolarWinds needed to, at a minimum, disclose their collective effect, especially in light of the Security Statement's positive portrayal of SolarWinds' cybersecurity practices.

1. SolarWinds and Brown Misleadingly Claimed to Follow the NIST Cybersecurity Framework for Evaluating Cybersecurity Practices.

74. In the Security Statement, SolarWinds and Brown claimed that the Company followed the NIST Cybersecurity Framework, claiming, "SolarWinds follows the NIST Cybersecurity Framework with layered security controls to help identify, prevent, detect and respond to security incidents." The NIST Cybersecurity Framework is a set of tools that an organization can use as one part of its assessment of its cybersecurity posture.

75. Companies using the NIST Cybersecurity Framework generally measure themselves on a scale of 0 to 5 in five main areas relating to cybersecurity: Identify, Detect, Protect, Respond, and Recover. Companies can also measure themselves on sub-areas of those five areas. These ratings are sometimes referred to as "NIST Scorecards" or "NIST Cybersecurity Scorecards."

76. In claiming to "follow" the NIST Cybersecurity Framework, Brown and SolarWinds made a materially false and misleading statement or omission by not revealing how poorly SolarWinds fared on multiple internal assessments using the Framework, including that

many of the supposed "layered security controls" were not in place at all. This started before the Relevant Period and continued at least well into 2019.

77. As detailed below, when evaluating its internal cybersecurity practices, through the NIST Cybersecurity Framework, or otherwise, SolarWinds consistently identified four critical areas that were particularly deficient: (1) secure development lifecycle; (2) network monitoring; (3) password protocols; and (4) access controls.

78. Additionally, as discussed below, many of the specific NIST Cybersecurity Framework controls that SolarWinds determined it was missing were controls that were important to securities analysts in determining whether investors should purchase SolarWinds stock.

a. SolarWinds' 2017 NIST Cybersecurity Framework Assessment Reveals Glaring Weaknesses.

79. In an August 9, 2017 email to Brown, Senior InfoSec Manager E wrote, "Here is my assessment of the state of our security program…." He attached an Excel workbook that contained NIST Cybersecurity Framework scores for many subareas within the five areas of Identify, Detect, Protect, Respond, and Recover, with each score separately broken out for SolarWinds' three main business units: CoreIT, MSP, and Monitoring Cloud.

80. Among the subareas rated as "0," meaning that "[t]here is no evidence of the organization meeting the security control objectives or [it] is unassessed" were the following:

- Identify – Business Environment (all three components)
- Protect – Awareness and Training (Monitoring Cloud)
- Detect – Security Continuous Monitoring (Monitoring Cloud)

81. Among the subareas rated as "1," meaning that "[t]he organization has an ad-hoc, inconsistent, or reactive approach to meeting the security control objectives" were the following:

- Identify – Risk Assessment (CoreIT and MSP)
- Protect – Awareness and Training (CoreIT and MSP)
- Protect – Data Security (all three components)
- Protect – Information Protection Processes and Procedures (MSP and Monitoring Cloud)

82. NIST Cybersecurity Framework scores of "0" and "1" are generally considered to be poor scores in the cybersecurity community.

b. SolarWinds' October 2018 NIST Cybersecurity Framework Assessment Shows Continued Weakness at the Time of the IPO.

83. An email from Senior InfoSec Manager E to several people including Brown that was sent on October 1, 2018, just weeks before SolarWinds' IPO, contained an updated assessment of SolarWinds' cybersecurity using the NIST Cybersecurity Framework. This Excel workbook contained even more detail than the 2017 assessment rated above, with scores not only for subareas, but specific controls—presumably representing the "layered security controls" referred to in the Security Statement. It also appears to refer to the component that had been "Monitoring Cloud" as simply "Cloud."

84. The subareas rated as "0" were the following:

- Protect – Maintenance (Cloud)
- Detect – Security Continuous Monitoring (Cloud)
- Detect – Detection Processes (Cloud)

85. Of the approximately 100 specific controls rated across the three areas (approximately 300 total), more than twenty-five specific controls were scored as "0," including:

- "Threat and vulnerability information is received from information sharing forums and sources" (Cloud)

- "The development and testing environment(s) are separate from the production environment" (Cloud)
- "Malicious code is detected" (Cloud)

86. Among the subareas rated as "1" were the following:

- Identify – Risk Assessment (Cloud)
- Protect – Awareness and Training (all three components)
- Detect – Anomalies and Events (Cloud)

87. More than fifty specific controls were scored as "1," including:

- "Asset vulnerabilities are identified and documented" (Cloud)
- "Access permissions are managed, incorporating the principles of least privilege and separation of duties" (all three components)
- "All users are informed and trained" (all three components)
- "Senior executives understand roles & responsibilities" (all three components)

88. Many of the low scores and missing / inconsistent controls listed above (or listed in the documents referred to above) directly contradict the Security Statement, as detailed below.

c. SolarWinds' 2019 NIST Cybersecurity Framework Assessment Reveals Ongoing Weaknesses.

89. Although Brown and his InfoSec team conducted NIST Cybersecurity Framework assessments in 2017 and 2018, it is unclear whether Brown or anyone on the InfoSec team alerted senior executives of the Company about the poor scores in 2017 and 2018. But at least as early as August 2019, a presentation to the CEO, whose metadata shows it was prepared by the CIO states it will "Introduce Security Score Card" (referring to the NIST Cybersecurity Framework Scorecard).

90. The 2019 NIST Cybersecurity Framework assessments presented to the senior executives contain significantly less detail than the 2017 and 2018 workbooks discussed above.

Still, SolarWinds had middling or poor scores in several critical areas, including a score of "2.0" for the "Recover" category (an apparent downgrade from the year before), a score of "2.0" for the subcategory of "Secure Software Development Lifecycle" and a score of "1.0" for the subcategory "Authentication, Authorization and Identity Management."

91. The poor results on NIST assessments from 2017 through 2019 discussed above were never disclosed to the public. SolarWinds' persistent poor scores, as alleged in this Amended Complaint, were not limited to an occasional or isolated instances; rather, the deficiencies reflected in these pervasive low scores, in critical areas, reflected widespread and years-long cybersecurity control deficiencies. SolarWinds misled the investing public by claiming to follow the NIST Cybersecurity Framework while omitting any reference to these scores, which is information necessary to make that statement not misleading.

d. A Separate NIST Assessment in 2019 Shows Critical Problems Persist Organization-Wide.

92. While the NIST Cybersecurity Framework can help provide a high-level view of an organization's cybersecurity, it is a general framework that does not contain detailed controls. Accordingly, organizations often choose more detailed NIST frameworks to help them implement or assess their cybersecurity practices.

93. NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations ("NIST 800-53") is one such detailed set of controls or protocols. SolarWinds' CIO testified that SolarWinds assessed its cybersecurity posture using the more specific set of controls in NIST 800-53.

94. NIST 800-53 includes "a set of cybersecurity activities, outcomes and informative references that are common across sectors and critical infrastructure" and is designed to "help an

organization align and prioritize cybersecurity activities with its business/mission requirements, risk tolerances and resources."

95. While publicly claiming that it followed the high-level NIST Cybersecurity Framework, SolarWinds failed to disclose that detailed internal assessments against the more specific NIST 800-53 framework showed many serious security gaps. Although the NIST Cybersecurity Framework and NIST 800-53 are separate protocols, SolarWinds CIO testified during the SEC's investigation that the Company used NIST 800-53 for scoring itself on the NIST Cybersecurity Framework scorecards that featured prominently in many internal presentations.

96. SolarWinds has now publicly stated that "[w]hether SolarWinds met NIST SP 800-53…has nothing to do with whether it followed the NIST [Cybersecurity Framework]." Regardless of whether the CIO was correct about her own department using NIST 800-53 in relation to the NIST Cybersecurity Framework, SolarWinds conducted a NIST 800-53 assessment in 2019 and the results revealed significant problems. Again, this was not an instance of a few missing controls, but of widespread and systemic failures in critical areas.

97. In mid-2019, documents show that SolarWinds used NIST 800-53 to evaluate whether certain of its products could be certified as compliant with the Federal Risk and Authorization Management Program ("FedRAMP"). In June 2019, Security & Compliance Manager L, under the supervision of Brown and the CIO, assessed current state at SolarWinds for the 325 NIST 800-53 controls (including controls relating to "identification and authentication," "access controls," and "incident response") to help determine the additional resources needed to achieve FedRAMP certification for those products.

98. Although the assessment was for specific products, many of the evaluated NIST 800-53 controls referred to organizational level-security practices. For example, one control evaluated asked whether "***The organization***…[m]onitors information systems for…atypical use …and [r]eports atypical usage of information systems accounts…" (SolarWinds did not). The results of the assessment were documented in attachments to emails that Security & Compliance Manager L sent to multiple people, including Brown on June 28, 2019 and August 28, 2019, and the CIO on September 25, 2019. They revealed multiple programmatic failures at an organizational level that directly contradict the Security Statement and placed SolarWinds at materially increased risk of a cybersecurity incident. Each failure or gap was prominently highlighted with a bright red box in the original document. Some of these specific findings are discussed in the sub-sections below regarding Secure Development Lifecycle, network monitoring, password management, and access controls.

99. In sum, in the 2019 FedRAMP/ NIST 800-53 assessments, SolarWinds identified having a "program/practice in place" for only 21 of the 325—or 6%—of NIST 800-53 controls, and "No program/practice in place" for 198 of the 325—or 61%—of the controls. The remaining 106 controls fell into the category of "Program/Practice *may* be in place but requires detailed review."

100. A subsequent assessment in April 2021 that was sent to Brown identified similar deficiencies, showed the percentage of "***completely unmet***" controls was nearly unchanged from 2019.

101. The undisclosed shortcomings in SolarWinds' NIST compliance rendered the Security Statement materially false and misleading. It contained information about the supposedly robust state of the Company's cybersecurity practices while omitting information

such as (a) SolarWinds' poor scores on the NIST Cybersecurity Framework five-point scale for certain critical subareas, (b) SolarWinds' NIST 800-53 assessment regarding organizational-level failures related to claims in the Security Statement, or (c) the other failures discussed below, some of which are not only omissions, but rendered specific representations in the Security Statement false.

102. Brown received the 2017 and 2018 NIST Cybersecurity Framework assessments, and at least two of the 2019 FedRAMP / NIST 800-53 assessments, all showing that there were many critical areas or controls where SolarWinds did not have a program or practice in place. These were not isolated instances of an employee failing to adhere to a policy, but systemic, organizational-level failures to employ adequate policies and procedures. Given his knowledge of the systemic, organizational-level failure to employ adequate policies and procedures, Brown knew, or was reckless or negligent in not knowing, that it was a materially misleading omission, if not an outright misstatement, for him and the Company to claim in the Security Statement that "SolarWinds follows the NIST Cybersecurity Framework with layered security controls to help identify, prevent, detect and respond to security incidents" without disclosing anything about the numerous failures and gaps documented in the assessments. But that statement remained on the SolarWinds' website throughout the Relevant Period.

e. SolarWinds and Brown's Misstatements and Omissions About the NIST Cybersecurity Framework, Were Material.

103. Reasonable investors considering whether to purchase or sell SolarWinds stock would have considered it important to know the true state of SolarWinds' cybersecurity practices because, among other reasons, poor cybersecurity practices could negatively impact sales and revenue, and therefore stock valuations. Cybersecurity practices are important to every publicly traded company. But they are especially important for a company like SolarWinds whose

primary product is not only software, but software that other organizations install to manage their own computer networks. As a result, cybersecurity disclosures are particularly material for SolarWinds.

104. SolarWinds also touted its compliance with NIST in multiple press releases that were posted and maintained on the investor portion of its website. This included a February 5, 2019 press release that touted that SolarWinds' "Technical requirements include FIPS compatibility, DISA STIGs, and National Institute of Standards and Technology (NIST®) government IT compliance" and a similarly worded March 21, 2019 press release regarding "National Institute of Standards and Technology (NIST®) compliance."

105. Securities analysts generally consider it important for companies to accurately disclose their risks. And for a company like SolarWinds that sold cybersecurity products, analysts consider it particularly important to accurately describe their cybersecurity risks and practices.

106. Multiple securities analysts who followed SolarWinds and other technology companies during the Relevant Period, including Analyst J and Analyst K, have confirmed that they considered it important that SolarWinds accurately disclose its cybersecurity risks and practices.

107. Brown himself stressed in a September 2020 blog post how important it was for software supply-chain vendors like SolarWinds to publicly issue—and follow—cybersecurity protocols:

> Over the past few years, security experts have increasingly emphasized the risks inherent in the software supply chain. Businesses rely on cloud applications that add complexity into an environment. The application itself could have bugs that leave an opening. Code libraries used by developers to simplify engineering could have flaws. The software could integrate with another application that may be insecure. In short, businesses do take on some additional risk in such an

> interconnected business environment. That's why it's important your software vendors take their roles as business partners seriously. Their security is your security. When looking for a vendor selling tools for your MSP—whether it's security tools, network management, or backup—it's important to not only match feature lists, but also kick the tires on their security. No software is perfect or vulnerability-free forever. But strong vendors put processes and protocols in place to reduce the risk and deal with threats if they crop up. And most importantly, strong vendors publish their security protocols and processes so you can evaluate whether they meet your standards. (If they don't, it's worth giving it a second thought on whether to trust them with your business and your data).

108. Brown similarly highlighted the importance of having (and touting) good cybersecurity practices in a May 2020 blog post, in which he advised SolarWinds' customers to "Emphasize your own security" and:

> …make sure you're taking care of your own house. Software companies often publish information on their own security practices to reassure customers. You can take a page from their book and mention your security policies in marketing materials, sales presentations, and website copy. As long as you practice sound security practices like patching, monitoring your systems, and using good password policies, consider making customers aware as a way of building trust.

109. Claiming to "follow" the NIST Cybersecurity Framework during the Relevant Period, without disclosing how poorly SolarWinds assessed itself regarding both that framework and the more detailed NIST 800-53 framework, was misleading and deprived investors of material information necessary to make the claim that SolarWinds followed the framework not misleading. A reasonable investor would have wanted to know that the true state of SolarWinds' cybersecurity practices left it far more vulnerable to a cyberattack than Solar Winds' public statements conveyed and that its cybersecurity practices could cause significant financial and reputational damage.

2. SolarWinds and Brown Falsely Claimed That the Company Followed a Secure Development Lifecycle When Creating Software for Customers.

110. In the publicly available Security Statement, SolarWinds and Brown claimed that the Company followed a "Secure Development Lifecycle" or "SDL." An SDL is a software

production methodology, developed by Microsoft, that standardizes industry best practices with the goal of creating secure software products. To follow an SDL, a company would employ numerous practices and controls, including training, threat modeling, penetration testing, and security testing. In the Security Statement, SolarWinds and Brown stated:

> We follow a defined methodology for developing secure software that is designed to increase the resiliency and trustworthiness of our products. Our products are deployed on an iterative, rapid release development lifecycle. Security and security testing are implemented throughout the entire software development methodology. Quality Assurance is involved at each phase of the lifecycle and security best practices are a mandated aspect of all development activities.
>
> Our secure development lifecycle follows standard security practices including vulnerability testing, regression testing, penetration testing, and product security assessments. The SolarWinds architecture teams review our development methodology regularly to incorporate evolving security awareness, industry practices and to measure its effectiveness.

111. Similarly, the public "Trust Center" of SolarWinds' website stated, "Secure Development Lifecycle. We follow a defined methodology to develop software designed to increase the resiliency and security of our products."

112. SolarWinds' internal SDL policy, which the CIO sent to Brown at least in November 2018, described multiple aspects of the SDL SolarWinds claimed to follow, including "Continuous Training," "Threat Modelling," "Secure Coding," and "Security Testing." The policy also claimed that "Prior to release the Final Security Review (FSR) assesses the complete security posture of the software system."

113. Additionally, SDL's "standard industry practices" (which SolarWinds publicly asserted it followed), included training and threat modelling, as set forth on the website of Microsoft Corp., the organization that developed SDL.[4]

[4] *See* https://www.microsoft.com/en-us/securityengineering/sdl/practices

114. Thus, Brown knew, or was reckless or negligent in not knowing, that when SolarWinds claimed to follow an industry-standard SDL, it implied, if not outright promised, to conduct training, threat modeling, security testing, and penetration testing. As discussed below, that was materially false and misleading.

a. In Truth, SolarWinds Pervasively Failed To Develop Software in a Secure Development Lifecycle During the Relevant Period.

115. SolarWinds pervasively failed to follow an SDL during the Relevant Period, including for components of the Company's "crown jewel" Orion platform that were ultimately used in the SUNBURST attack. Instead, SolarWinds and Brown knew, or were reckless or negligent in not knowing, that the Company was still working to determine how to incorporate aspects of an SDL into its product development leading up to and throughout the Relevant Period.

i. The Security Statement's Description of SolarWinds' SDL Practices Was False When Brown Wrote It.

116. The Security Statement's false promises that SolarWinds followed an SDL were part of a pattern and practice of SolarWinds making "aspirational" statements about its cybersecurity—statements that represented what SolarWinds hoped to do someday—and falsely portraying them as what SolarWinds actually did at the time.

117. For example, in a January 2018 email to multiple senior managers, including SolarWinds' CIO, Engineering Manager H bluntly admitted that the Security Statement's SDL section was false. Engineering Manager H had alerted multiple engineering managers about SolarWinds' "public facing" security statement, and specifically called attention to its statements regarding SDL. A few days later he admitted that "I've gotten feedback that we don't do some of the things that are indicated in the [Security Statement SDL Section]." Rather than suggest amending the Security Statement to make it accurate, Engineering Manager H explained that

SolarWinds would continue to hide the falsity of these statements and work toward making them eventually true: "I want to make sure that you all have an answer to this. The simple response is: There is improvement needed to be able to meet the security expectations of a Secure Development Lifecycle. We will be working with teams throughout 2018 to begin incorporating the SDL into their development lifecycle." The email then described a plan that "begins with general SDL training" and described deploying SDL "pilots" and working to "roll out the SDL to additional teams each quarter." A plan to begin taking steps to implement an SDL is a far cry from presently employing an SDL, which is what SolarWinds and Brown represented to the public: "Our secure development lifecycle follows standard security practices…"

118. Additionally, Engineering Manager H's statement to multiple senior managers that SolarWinds was not doing what it was publicly saying it was doing in the Security Statement and that it should attempt to start doing what it publicly claimed it had already shows that from when the Security Statement was first posted it was a knowing deception of customers and the investing public. Even when multiple senior managers were made aware that it was false, it was not corrected. Indeed, it does not seem that the idea of correcting it was even discussed.

119. Another email from Engineering Manager H, in May 2018 to Brown and SolarWinds' CIO, sounded a similar theme: "[Threat Modeling] is a process. It's part of the SDL and we are just barely beginning to understand how teams are going to be doing this activity." These emails are evidence of a scheme, act, practice, or course of business to conceal the true state of SolarWinds' cybersecurity practices from both its investors and customers. That scheme continued well into the Relevant Period, as Brown was repeatedly made aware that SolarWinds was failing to do essential parts of an SDL. But the Security Statement never changed during the Relevant Period.

ii. The Security Statement's Representation that SolarWinds Followed an SDL Remained False During the Relevant Period.

120. As discussed above, utilizing an SDL includes conducting "Security Testing" and "Penetration Testing,"[5] and SolarWinds and Brown specifically stated that SolarWinds did both types of testing: "Our secure development lifecycle follows standard security practices including vulnerability testing, regression testing, penetration testing, and product security assessments." At least for significant portions of the Relevant Period, that was false, as SolarWinds often noted its failure to conduct such testing.

121. A presentation for the annual offsite meeting with SolarWinds' CEO admitted that Penetration testing was unfunded in 2018. And the presentation from December 2018 whose metadata indicates it was prepared by Senior InfoSec Manager E also stated in "Key Areas to Address Gaps in Information Security" that for "Product Penetration Testing" there was "No formalized testing. Identify and integrate penetration testing into product development phases."

122. SolarWinds' internal policy pertaining to SDL required that products like the Orion Improvement Program which store, process, or manage data, must be scanned for vulnerabilities and security tested before their release. And the Security Statement represented that SolarWinds conducted security testing prior to releasing products. But a July 2020 internal presentation prepared by Brown and reviewed by SolarWinds' CIO and SolarWinds' CTO admitted, "Inconsistent internal security testing as part of product final security reviews don't always include web application testing before release."

123. Threat modelling and continuous security training are essential to implementing an industry standard SDL. As discussed above, SolarWinds claimed to follow standard practices.

[5] NIST defines Penetration Testing as "A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of a system."

But Brown had documented SolarWinds' failure to have security training as far back as the August 2017 Security State of the Union, and the failures continued for years. At least in 2018 and 2019, SolarWinds still failed to have training or threat modelling in place for large and important segments of its business.

124. In the October 2018 NIST Cybersecurity Framework assessment discussed above, multiple specific controls regarding training and threat modelling were rated "0" or "1." This included "Threat and vulnerability information is received from information sharing forums and sources" which was rated as "0" for Cloud services; "Threats, both internal and external, are identified and documented," which was rated "1" for Cloud services; "All users are informed and trained," which was rated "1" for all three business segments; and "Privileged users understand roles & responsibilities," which was rated "1" for all three business segments.

125. During the Relevant Period, one of SolarWinds' business units was the Managed Service Provider, or MSP, unit that focused on Managed Service Providers, companies that used SolarWinds' products to provide network management services to end users. Those end users often included small or medium-sized companies that wished to outsource their network management. Brown considered the MSP business to be one of SolarWinds' "crown jewels."

126. A July 2019 "MSP Products Security Evaluation" whose cover indicates it was prepared by a SolarWinds engineer and whose metadata lists Security & Compliance Manager L as the custodian, assessed "the operational maturity level" for several "key" MSP products. It appears to evaluate both the cybersecurity of the products and the cybersecurity of the Company (or at least the portion of the Company dedicated to MSP products) using the NIST Cybersecurity Framework (confusingly referred to in the document as "NIST, the Enterprise

standard security Framework"). Several of the many cybersecurity problems flagged in this document are listed below, including failures in training and threat modelling:

- Documentation for communication and data flows was lacking and unstructured for the majority of products. "These are crucial for threat modelling & other security activities in SSDLC.[6] This should be covered by architecture, as part of the SSDLC process being formed."[7]
- Each product seems to have its own ways of marking security issues that do not follow recently established [SolarWinds] standards.
- "No threat modelling nor analysis is performed as part of any process (except MSP Backup Engineering)."
- There is no security awareness training as well; there is no security training during the onboarding process.

127. A similar MSP Products Security Evaluation for a different "key" MSP product in December 2019, which appears to have been drafted by the same engineer and whose metadata lists Brown as the custodian, sets forth many similar problems, including that:

- Documentation for communication and data flows is lacking and unstructured…"These are crucial for threat modelling & other security activities in SSDLC.[8] This should be covered by architecture, as part of the SSDLC process being formed."[9]
- "No threat modelling nor analysis is performed as part of any process…."
- "There is no security awareness training as well there is no security training during onboarding process."

128. An August 16, 2019 Security and Compliance Program Quarterly Overview presentation listed "Secure Software Development Lifecycle" with an objective of "Employees are aware of [and] utilize a security software development lifecycle in their day to day activities" as only having a score of 2 on the NIST Cybersecurity Framework Five-Point scale, meaning it was an area where SolarWinds "has a consistent overall approach to meeting the security control

[6] "SSDLC" here may be a reference to SDL.
[7] Unless in quotation marks, information in the bullet points in this paragraph are paraphrased.
[8] SSDLC here may be a reference to SDL.
[9] Unless in quotation marks, information in the bullet points in this paragraph are paraphrased.

objectives, but it is still mostly reactive and undocumented. The organization does not routinely measure or enforce policy compliance." Brown was responsible for the cybersecurity content in the Security and Compliance Program Quarterly Overview presentations during the Relevant Period.

129. In the 2019 FedRAMP / NIST 800-53 assessments that were sent to Brown and the CIO (as discussed above), for each of the five "Awareness and Training" controls that were evaluated, Security & Compliance Manager L determined that "[w]e have incident commander training however, not a security training/awareness program in place."

130. Those FedRAMP / NIST 800-53 assessments also admitted that SolarWinds was still only at the stage of having a "[p]rogram in the works" for threat modelling, in connection with the control "[t]he organization requires the developer of the information system, system component, or information system service to perform threat and vulnerability analyses and subsequent testing/evaluation of the as built system, component, or service…"

131. In June 2020, in connection with the U.S. Government Agency A incident (detailed below), a SolarWinds engineer questioned by email whether the Orion Improvement Program ("OIP"), a component of the Orion platform, was developed under an SDL process. "Do we have [sic] SDL process enforced for Orion Improvement Program server? If SDL is not enforced for OIP, we should do it ASAP and consider additional actions to make sure that OIP is very well protected." Another engineer responded, "I don't believe we cover OIP today with the SDL, but we should." The email was forwarded to SolarWinds' CIO and Brown.

132. One reason the engineer questioned whether OIP was under the SDL was because he had determined it was using a library of software code that he described as "vulnerable," and which was listed in the U.S. Department of Commerce National Institute of Standards and

Technology's National Vulnerability Database (also known as the Common Vulnerabilities and Exposures Program). The engineer even provided a weblink to that database's entry for the library's known vulnerability. That entry, still accessible on the NIST National Vulnerability Database, indicates that it was last modified in 2019 and describes the library as "vulnerable to directory traversal," meaning threat actors with access to one part of a system could more easily access another part of the system.

133. Brown confirmed in sworn testimony that the OIP was not built under an SDL process in 2020, and emails show he was aware of this fact at the time.

134. The issues outlined above were not isolated instances where a small group of employees missed a training session, or a single instance of failing to employ threat modelling. Rather, they represent a continuous, systemic failure—lasting from at least January 2018 to at least July 2020—to implement the SDL that SolarWinds claimed to follow.

135. The Security Statement remained false and misleading throughout the Relevant Period. It was never updated during the Relevant Period to reflect any of these SDL issues or failures, nor did SolarWinds or Brown otherwise publicly disclose these ongoing issues or failures.

b. SolarWinds and Brown's Misstatements and Omissions Regarding a Secure Development Lifecycle Were Material.

136. The Company's false and misleading statements about its SDL during the Relevant Period were not only false and misleading, but materially so. A reasonable investor, considering whether to purchase or sell SolarWinds stock, would have considered it important to know the true state of SolarWinds' security regarding product development, especially regarding the development of portions of a "crown jewel" product like Orion or the MSP products. But the

Security Statement's misrepresentations about developing products using SDL deprived investors of that material information.

137. Analyst J and Analyst K confirmed to the SEC staff that they viewed a failure by a large software development company to follow the SDL in creating its products an important fact that they would want to know about before recommending that investors purchase or sell the company's stock.

i. Failing to Utilize an SDL Put SolarWinds' "Crown Jewels" at Risk.

138. Brown admitted the importance of companies following an SDL and maintaining a secure environment for all software products they develop in a September 2020 blog post:

> …try to inquire about how organizations develop their code. For example, some organizations implement the Secure Development Lifecycle [SDL], a framework standardized by US-CERT. Following these practices increases the likelihood of producing secure products. The [SDL] includes several components and practices for understanding security requirements, developing code securely, testing before code deployment, and incident response for issues that occur. (If you're curious and want to take a deep dive into the [SDL], visit US-CERT.) The most important takeaway here, however, is that organizations should have a strong, mature model for developing secure products and maintaining their own security.

139. Moreover, in a September 2019 interview, Brown stressed the importance of a company protecting its "crown jewels" from a cybersecurity attack, and described failing to do so as an "extinction event":

> Enterprises, it is a choice. It is a risk choice that they have made to say 'Here is my budget. Here is what I'm going to spend on security. Hopefully, I've done a good job. Here are my crown jewels. I understand what would be an extinction event for me and I'm protecting against those.'
>
> * * *
>
> My broad-based mission is to basically eliminate anything that is material damage to my company. I know I can't eliminate everything. So, that's the first rule. So what do I eliminate that would be materially damaging to my company?

140. Similarly, in an August 25, 2020 podcast, Brown claimed that companies needed even higher protection around their crown jewels:

> It's super key that you understand your crown jewels essentially, understand your mission and business critical application. So important to be able to understand what the most important assets in your environment are, and then protect them at a different level than what you protect everything else.

141. But not only did SolarWinds fail to utilize an SDL, it failed to do so for its crown jewel products, including its MSP products and at least the OIP portion of the Orion platform.

ii. SolarWinds and Brown's Misstatements Regarding Security Training Were Material.

142. Not only was the overall failure to implement SDL material, but at least some of the reasons that SolarWinds failed to implement an SDL were also material by themselves. In a February 2019 article, Brown was quoted as explaining that training was critical for maintaining security:

> Untrained staff, unmitigated access and lack of good policies are all big contributors to security vulnerabilities. Make sure you've taken the time to establish policies, and train anyone and everyone who has access to your systems. And, make sure that you haven't granted that access too widely. The bad guys can get to your 'crown jewels' easily, for example, by throwing out a phishing line to an HR administrator if that administrator's credentials aren't locked down tightly.

143. Brown made similar comments in a March 2019 blog post, lecturing SolarWinds' MSP customers that "you must do your best to not only offer security trainings but make them engaging so your customers' employees retain the information and, hopefully, think twice before putting the Company at risk." But at the same time, as shown above, SolarWinds was not conducting security awareness trainings for its own MSP business segment, and possibly not anywhere in the Company.

144. Analyst J and Analyst K also confirmed that a lack of security awareness training at SolarWinds (at least if it persisted for a lengthy period of time) was a fact that they would consider important in deciding whether to recommend purchasing or selling SolarWinds stock.

iii. SolarWinds and Brown's Misstatements Regarding Threat Modelling and Testing Were Material.

145. Analyst J confirmed that threat modelling was particularly important for a company that develops software. He also confirmed that a lack of penetration testing by SolarWinds in 2018 was a fact that he would consider important in deciding whether to recommend purchasing or selling SolarWinds stock. Analyst K similarly confirmed that he assumed a large software development company like SolarWinds would do things like threat modelling and security testing on their products before releasing them. And Analyst K confirmed that if SolarWinds had persistent failures to do those things, he would have considered it important in his evaluation of the Company's stock.

146. Additionally, the lack of penetration testing in this earlier timeframe is particularly concerning, because later penetration testing revealed numerous vulnerabilities. For example, a September 2020 penetration test of the core MSP product, N-Central, contained the following overall finding in the executive summary: "The overall technical risk for N-Central based on the Web Application Penetration Test and the impact of the discovered vulnerabilities is ***High***" (emphasis in original).

147. As discussed above, Brown knew that, at least from 2018 through 2019, SolarWinds (1) did not have adequate security training, (2) did not conduct threat modelling, and (3) did employ adequate security testing before product release. Each of those is essential to utilizing an SDL. Given his knowledge of the systemic, organizational-level failure to employ adequate policies and procedures, Brown knew, or was reckless or negligent in not knowing, that

it was materially misleading for him and the Company to claim in the Security Statement that "[o]ur secure development lifecycle follows standard security practices including vulnerability testing, regression testing, penetration testing, and product security assessments." But that misleading statement remained on SolarWinds' website throughout the Relevant Period.

3. SolarWinds Falsely Claimed to Monitor Its Networks.

148. In the Security Statement, SolarWinds falsely claimed to monitor its networks in several ways:

> **Change Management**
>
> Changes to information systems, network devices, and other system components, and physical and environment changes are monitored and controlled through a formal change control process. Changes are reviewed, approved, tested and monitored post-implementation to ensure that the expected changes are operating as intended.
>
> **Auditing and Logging**
>
> Network components, workstations, applications and any monitoring tools are enabled to monitor user activity.
>
> **Network Security**
>
> Our infrastructure servers reside behind high-availability firewalls and are monitored for the detection and prevention of various network security threats…Next generation firewalls deployed within the data center as well as remote office sites monitor outbound communications for unusual or unauthorized activities…

a. In Truth, SolarWinds Had Long-standing Network Monitoring Failures.

149. As shown below, SolarWinds documented numerous issues with network monitoring over years. The 2017 NIST Cybersecurity Framework assessment described above scored "Security Continuous Monitoring" as "0" for the "Monitoring Cloud" business segment. Again, that meant that "There is no evidence of the organization meeting the security control objectives or is unassessed."

150. The 2018 NIST Cybersecurity Framework discussed above also scored "Security Continuous Monitoring" as "0" for the Cloud business segment, and downgraded "Detection Processes" for Cloud to "0" from its "3" score the year earlier.

151. Among the specific controls the 2018 NIST Cybersecurity Framework scored as "0" related to network monitoring were these controls for the Cloud business segment:

- "The network is monitored to detect potential cybersecurity events"
- "Personnel activity is monitored to detect potential cybersecurity events"
- "Malicious code is detected"
- "Unauthorized mobile code is detected"
- "External service provider activity is monitored to detect potential cybersecurity events"

152. Likewise, a September 2018 presentation on "Information Security" that was sent from Brown to the CTO used red font to flag that "Active monitoring and true SOC services" were "Limited or non existent"

153. The 2019 FedRAMP / NIST 800-53 assessments sent to Brown and the CIO revealed similar organizational failures. For the control "[t]he organization…[m]onitors information systems for…atypical use…and [r]eports atypical usage of information systems accounts…" the assessment was "GAP. Currently there is no program for this across [SolarWinds]." And for the control "[t]he organization develops a continuous monitoring strategy and implements a continuous monitoring program…" the assessment was "[w]e have no continious [sic] monitoring in place."

154. These were not isolated Network Monitoring failures, but represented a systemic, undisclosed problem at SolarWinds that rendered the Security Statement materially misleading.

b. **The Misstatements Regarding Network Monitoring Were Material.**

155. Network monitoring is vital to good overall cybersecurity. Among other things, it can help prevent or detect threat actors seeking to move laterally within a computer network or exfiltrate files from a network.

156. In a January 22, 2020 blog post, Brown acknowledged the importance of network monitoring when admonished SolarWinds customers to do it:

> If you own an MSP, you probably offer some security measures to your customers already, but you can't skimp on your own—your security must be stronger than your customers'. There are several steps you can take to reduce your risk of a breach. While nothing's bulletproof, these steps can help reduce your overall danger.

Brown then listed steps that should be taken, including the "fundamental[]" step of "protect and monitor your network by using a next generation firewall," and more advanced monitoring techniques (plus training, password security, and others).

157. Analyst K confirmed that he would have considered it important in his evaluation of SolarWinds stock if he had learned that SolarWinds had widespread and persistent failures regarding network monitoring.

158. Brown received the 2017 and 2018 NIST Cybersecurity Framework assessments, and at least two of the 2019 FedRAMP / NIST 800-53 assessments, all showing that there were many critical network monitoring failures. These were not isolated instances of an employee failing to adhere to a policy, but systemic, organizational-level failures to employ adequate policies and procedures. Given his knowledge of the systemic, organizational-level failure to employ adequate policies and procedures, Brown knew, or was reckless or negligent in not knowing, that it was a materially false and misleading for him and the Company to claim in the Security Statement that "[o]ur infrastructure servers reside behind high-availability firewalls and

are monitored for the detection and prevention of various network security threats" without disclosing anything about the many failures and gaps documented in the assessments. But that statement remained on the SolarWinds' website throughout the Relevant Period.

4. SolarWinds and Brown Falsely Claimed that SolarWinds Implemented a Strong Password Policy.

159. SolarWinds' Security Statement falsely claimed the Company not only had, but enforced, a strong password policy. SolarWinds and Brown stated:

> We require that authorized users be provisioned with unique account IDs. Our password policy covers all applicable information systems, applications, and databases. Our password best practices enforce the use of complex passwords that include both alpha and numeric characters, which are deployed to protect against unauthorized use of passwords.

160. SolarWinds' password policy, which was incorporated by reference in the Security Statement, required passwords to (1) be changed every 90 days, (2) have a minimum length of eight characters, and (3) include three of the four following characteristics: upper case letter, lowercase letter, base-10 digit (0-9), and non-alphanumeric character.

161. Solar Winds' Security Statement also stated that "Passwords are individually salted and hashed." The phrase "individually salted and hashed" meant that the passwords were maintained in an encrypted state.

162. As discussed below, these statements were materially false and misleading.

a. In Truth, SolarWinds Failed to Enforce or Comply With Its Own Password Policy on Multiple Occasions.

163. Contrary to its Security Statement, SolarWinds did not enforce strong password requirements on all of its information systems, applications, and databases, as Brown and SolarWinds knew or were reckless or negligent in not knowing. Indeed, throughout the Relevant Period, multiple instances of password problems were flagged for Company management, but

the Company let password problems persisted for years, as shown in numerous internal documents, including those discussed below.

164. In an April 2017 email to the newly hired CIO, a SolarWinds employee expressed surprise that things "like 'default passwords' are [still] plaguing us when the product has been in the market [this long,]" explaining, "[m]any of these vulnerabilities seem pretty well amateur hour." As an example, the employee identified one SolarWinds product for which the default password was "password." Senior InfoSec Manager E testified that having a default password of "password" is a "poor security practice."

165. An April 2018 audit shared with SolarWinds' CIO identified multiple critical systems that did not comply with the password policy. The audit found systems where "shared SQL legacy account login credentials [were] used," contrary to the Security Statement's claim that SolarWinds "require[s] that authorized users be provisioned with unique account IDs."

166. That same April 2018 audit also found database passwords that were "not encrypted within the configuration file," login credentials that were "stored in plain text in configuration files," and passwords that were "stored in plain text on the public web server in the web configuration file and in the system registry of the machine." In other words, the passwords were not individually stored in an encrypted state or "salted as hashed," as SolarWinds and Brown represented in the Security Statement. All of these issues flagged in the April 2018 audit were described as high risk.

167. Password problems continued well into the Relevant Period. Sarbanes-Oxley ("SOX") audits in 2019 and 2020 documented additional instances in which "[p]assword requirements" and "password history" requirements were not met. At least some of these deficiencies were brought to the attention of senior management. For example, SolarWinds' CFO

was aware that for 2019, of the 100 Information Technology General Controls tested for SOX purposes, 27 were found to be deficient. Of those 27 deficient controls, 10 were still unremediated by March 2020, including multiple access and password controls.

168. SolarWinds used Quarterly Risk Review presentations that were compiled by Brown and others in the Company's Information Technology group to highlight the current information technology status and risks. They were routinely shared with the CIO, CTO, and other senior executives. A March 2020 email and Quarterly Risk Review presentation drafted with input from Brown and shared with SolarWinds' CIO and CTO (who then updated SolarWinds' CEO), described findings from SolarWinds' SOX audit of internal controls. That included "SOX Control Deficiencies" such as situations where "[p]assword requirements [were] not met."

169. Passwords for other systems at the Company likewise fell well short of its stated password policy. A September 2019 email from a SolarWinds compliance employee to SolarWinds' CIO described security risks for the main source of authentication for SolarWinds' Cloud product line. Specifically, the compliance employee observed that "Passwords have no specific parameters, as stated in the IT guidelines"; and "Passwords are able to be reused and are not changed at a set number of days." This was both a product issue and an internal security issue because employees in SolarWinds' IT and Development Operations groups used the Company's cloud-based products in their jobs at SolarWinds and authenticated through the system.

170. In the 2019 FedRAMP / NIST 800-53 assessments (discussed above), the 300+ controls were broken down into sub-categories and assessed as either having "Program/Practice in place," "Program / Practice may be in place but requires detailed review," or "No program /

practice in place." For the subcategory "Identification and Authentication" zero controls were rated "in place," seven were rated as "may be in place" and twenty controls had "No program/practice in place."

171. Again, while the 2019 FedRAMP / NIST 800-53 assessments were done for certain products, many of the controls were evaluated Company-wide. For example, the assessments asked whether "***The organization*** employs automated tools to determine if password authenticators are sufficiently strong…" (emphasis added). SolarWinds determined that it had "No known automated tools for [password] authentication."

172. During the Relevant Period, SolarWinds used an Akamai server to distribute software updates to its customers. In November 2019, an outside security researcher notified SolarWinds that the password for the Company's Akamai server was publicly available, and that a threat actor could use that public password to infect SolarWinds' software updates: "I have found a public Github repo which is leaking ftp credential belong[ing] to SolarWinds…. Via this any hacker could upload malicious exe [executable code] and update it with release [of] SolarWinds product." Senior InfoSec Manager E confirmed the security researcher's description. The password that was publicly available was "solarwinds123," an astonishingly simple password that did not comply with the Company's stated password complexity requirements.

173. The Security Statement was never updated during the Relevant Period to reflect any of these password issues or failures, but instead continued to state that "[o]ur password best practices enforce the use of complex passwords that include both alpha and numeric characters, which are deployed to protect against unauthorized use of passwords." Nor did SolarWinds or Brown otherwise publicly disclose these issues or failures.

b. SolarWinds and Brown's Misstatements and Omissions Regarding SolarWinds Password Policy Were Material.

174. SolarWinds and Brown's false and misleading statements and omissions regarding password issues were not only false and misleading, but materially so. A reasonable investor, considering whether to purchase or sell SolarWinds stock, would have considered it important to know the true state of SolarWinds' password policies, especially considering that these issues were long-standing and potentially affected customer-facing areas such as the Akamai server used to send updates to customers.

175. Brown recognized the importance of such password issues in a September 2019 interview:

> Enterprises that get breached. That was their choice. It seriously was. It was 100 percent their choice. If you look at the attacks that have been successful, most of them have been silly mistakes. Passwords that were stored in the wrong way. Machines that were vulnerable. Systems that weren't patched.

176. Similarly, a May 2020 article on information-age.com for World Password Day identified Brown as vice president of security at SolarWinds MSP and quoted him regarding the importance of strong password policies and access controls:

> Simple standalone passwords may be easy to remember, easy to use, and work across many environments, but they are also easy to guess, easy to phish, and easy to compromise…you should always go to the next step beyond complex passwords with multi-factor authentication or conditional access, especially for sensitive environments.

177. Brown received at least two of the 2019 FedRAMP / NIST 800-53 assessments and compiled the Quarterly Risk review presentations, all showing that there were multiple password failures. Viewed together, these were not isolated instances of an failing to adhere to a password policy, but systemic, organizational-level failures to employ adequate policies and procedures. Given his knowledge of the systemic, organizational-level failure to employ adequate policies and procedures, Brown knew, or was reckless or negligent in not knowing, that it was a

materially false and misleading for him and the Company to claim in the Security Statement that "[o]ur password best practices enforce the use of complex passwords that include both alpha and numeric characters, which are deployed to protect against unauthorized use of passwords." But that statement remained on the SolarWinds' website throughout the Relevant Period.

5. SolarWinds and Brown Falsely Claimed That the Company Maintained Strong Access Controls.

178. SolarWinds described "Access Management" as "the management of individual identities, their authentication, authorization, roles and privileges within the enterprise in order to minimize security risks associated [sic] the use of privileged and non-privileged access." Individuals at the Company used the phrases "access management" and "access controls" interchangeably. Password policies can be considered one part of access controls, but access controls also include other policies such as what rights or privileges a user has and for which portions of a company's computer network. For example, a person with "administrator" or "admin" rights typically has broader privileges to make significant changes to the software in a given area, such as changing security settings, installing software and hardware, accessing all files on the computer, and making changes to other user accounts.

179. SolarWinds' Security Statement included a section regarding "Access Controls" in which Brown and SolarWinds claimed that SolarWinds implemented strong Access Control policies:

> Role based access controls are implemented for access to information systems. Processes and procedures are in place to address employees who are voluntarily or involuntarily terminated. Access controls to sensitive data in our databases, systems, and environments are set on a need-to-know / least privilege necessary basis. Access control lists define the behavior of any user within our information systems, and security policies limit them to authorized behaviors.

The statement continued:

> SolarWinds employees are granted a limited set of default permissions to access company resources, such as their email, and the corporate intranet. Employees are granted access to certain additional resources based on their specific job function. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as defined by our security guidelines. Approvals are managed by work-flow tools that maintain audit records of changes.

180. As discussed below, these statements were materially false and misleading.

a. In Truth, SolarWinds Had Allowed Significant Access Problems to Persist for Years.

181. SolarWinds' actual access control environment was diametrically different from the description in the Security Statement. SolarWinds had poor access controls—a problem that it failed to remedy for years. Among other things, SolarWinds and Brown claimed in the Security Statement that employees had access on a "least privilege necessary basis." The concept of "least privilege" is an industry-standard concept that persons should be granted the minimum system resources and authorizations needed to perform their job functions. SolarWinds and Brown further represented, "Role based access controls are implemented for access to information systems," and "SolarWinds employees are granted a limited set of default permissions to access company resources."

182. In reality, from at least 2017 through at least 2020, as Brown and SolarWinds' senior management knew, or were reckless or negligent in not knowing, SolarWinds routinely and pervasively granted employees unnecessary "admin" rights, giving them access and privileges to more systems than necessary for their work functions and violating the concept of "least privilege." Indeed, there is evidence that most employees had "admin" rights at times during the Relevant Period.

183. Internal Company assessments identified numerous access control violations, including expansive use of "admin" privileges and a virtual private network security gap that was exacerbated by the Company's failure to enforce its remote access policies.

184. A June 2017 presentation prepared by SolarWinds' Director of IT and shared with its CIO described an "unnecessary level of risk" from too many accounts having admin level access, including the "[s]ystem team" using admin accounts during routine operations.

185. Brown's August 2017 Security State of the Union warned of the need to "Lock down administrative access."

186. A January 2018 presentation prepared by a SolarWinds project manager and shared with Brown, as well as SolarWinds' CIO, Director of IT and others, warned that "Currently there is a collection of people who have access to many systems and many people involved in provisioning access." The presentation specified that the "lack of standardized user access management processes…create a loss risk of organizational assets and personal data."

187. Brown and Senior InfoSec Manager E prepared a March 2018 Security Projects slide presentation and provided it to SolarWinds' CIO. That presentation warned that the "[c]oncept of least privilege [is] not followed as a best practice" and described the "[u]se of shared accounts throughout internal and external applications."

188. An April 2018 audit (referred to above) set forth that "Non-privileged accounts [were] being granted local administrator permissions on server." Again, this was flagged in the audit as a "High" risk.

189. A September 2018 presentation on "Information Security" that was sent from Brown to the CTO used red font flag that "Identity Management - Role and Privilege management" was "Limited or non existent."

190. A different September 2018 Presentation whose metadata indicates that the CIO was the custodian entitled "Bi-Weekly DOIT Staff Meeting" included a slide titled "SOX Controls: Findings Summary" whose subtitle was "#notwinning" and documented that for "User Access Management" of the 7 controls reviewed only 3 were in place with 4 "Partially in Place." A frowny-face emoji appears next to this assessment.

191. The presentation from December 2018 whose metadata indicates it was prepared by Senior InfoSec Manager E also listed in "Key Areas to Address Gaps in Information Security" that SolarWinds still needed to "Define standards and best practices for Role Based Access Controls and Least Privilege" and "Address the use of local administrator access to non-privileged users. Manage, audit, and apply security controls around privileged access."

192. An August 2019 Security & Compliance Program Quarterly Review that Brown prepared, the CIO reviewed, and the CEO received, acknowledged, "Access and privilege to critical systems/data is inappropriate." That same presentation highlighted the need to improve internal practices and procedures. And it assessed that for "Authentication, Authorization and Identity Management," where the control objective was "User identity, authentication and authorization are in place and actively monitored across the company," SolarWinds had a NIST Cybersecurity Framework score of 1. That meant the Company had an ad-hoc, inconsistent, or reactive approach to meeting that cybersecurity control objective.

193. The same 2019 internal FedRAMP / NIST 800-53 security controls assessments that were sent to Brown and the CIO (discussed above) also assessed the subcategory "Access controls." That subcategory contained forty-three controls, with just two rated "in place," eighteen rated "may be in place," and twenty-three rated "No program/practice in place." Of those forty-three evaluated access controls, six related specifically to the concept of least

privilege. Of those six least privilege controls, SolarWinds had "No program/practice in place" for four. The other two noted: "This is included in the Access/Security Guidelines document. An audit that this is in place has never been performed."

194. Among the controls that were not in place were several that rendered SolarWinds' and Brown's statements about access controls materially false and misleading, as shown by the chart below:

Control Evaluated	**Finding**
"The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on…organization-defined information flow control policies"	"Agree with [Product Manager]. This is a gap"
"The organization explicitly authorizes access to…organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information…Security functions include, for example, establishing system accounts, configuring access authorizations (i.e., permissions, privileges)…"	"We have no explicit authorization policy, nor is this documented that I am aware of for the company or individual products"
"The organization restricts privileged accounts on the information system to…organization-defined personnel or roles…"	"We have no explicit restriction policy, nor is this documented that I am aware of for the company or individual products"
"The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures."	"This has not been tested/audited, nor is a policy documented."
"The organization: (a) Limits privileges to change information system components and system-related information within a production or operational environment; and…"	"No known privledge [sic] limitations"

195. The lack of the controls in chart above corroborates multiple documents and witnesses that identified the extensive granting of administrative privileges to many employees as a widespread problem at the Company during the Relevant Period. It also directly contradicts the claims in the Security Statement that (1) SolarWinds provisioned access on a least privilege

necessary basis, (2) employees were granted a limited set of default permissions, and (3) the granting of greater permissions followed a formalized approval process.

196. The access control problems continued into late 2019 and beyond. A September 18, 2019 email from a SolarWinds compliance employee to Brown and SolarWinds' CIO also identified multiple cybersecurity deficiencies associated with the main source of authentication for SolarWinds' Cloud product line. This authentication source was both a SolarWinds product sold to customers, and a product that SolarWinds used internally on its own systems by employees in the IT and Dev[elopement] Op[eration]s groups who used the Company's Cloud-based products in their jobs at SolarWinds. Thus, failures in it affected SolarWinds both from a product perspective and an internal cybersecurity perspective. (SolarWinds used many of its own products internally). Here, the compliance employee observed that "passwords have no specific parameters" in violation of policy, that "access is not audited nor monitored," and that multiple problems existed with product development requirements. In all, the email assessed that 27% of security controls for the product were unmet. In testimony, the CIO confirmed that access control deficiencies in the authentication system could create cybersecurity risks for SolarWinds, while noting that there might have compensating controls in place.

197. A November 2019 presentation whose metadata lists Security & Compliance Manager L as its custodian detailed numerous additional access control problems related to SolarWinds' MSP Support Portal including:

a) "MSP Support staff has a significant level of system level access to both MSPs and MSP customers. The level of access is excessive and if abused poses a significant insider threat. Currently, a support person has the ability to gain privileged access, connect or run procedures on one or more MSPs and their customer environments."

b) For some software, "Support staff has access to usernames and passwords for all MSP distributors and customers."

c) For another set of software, "Support staff has access to a distribution portal that enables access directly to customer's environments. We have not seen any cases of this type of abuse from the support team but if an adversary was looking to circumvent our security an insider attack would be one of the easiest to perform."

d) "Recent incidents have involved support staff and engineering's inappropriate access to customers environments."

e) And the presentation flagged that changing this was necessary in order to align with the concept of "least privilege."

198. As discussed above, Brown helped draft Quarterly Risk Review presentations that sometimes highlighted cybersecurity issues to SolarWinds' senior executives. For example, Quarterly Risk Review presentations in March and October 2020 were drafted with input from Brown and shared with SolarWinds' CIO and CTO, who in turn updated SolarWinds' CEO. Those presentations acknowledged "[s]ignificant deficiencies in user access management." Nonetheless, at times or concerning certain specific issues, Brown failed to ensure that other senior executives were sufficiently aware of, or understood, the severity of cybersecurity risks, failings, and issues that he and others knew about. These failures were exacerbated by the Company's poor or inadequately maintained disclosure controls.

199. Again, the Security Statement remained materially false and misleading throughout the Relevant Period as it never accurately reflected the true state of SolarWinds' access controls, including any of these access control issues or failures described above, nor did SolarWinds or Brown otherwise publicly disclose the existence of significant deficiencies in the Company's access controls that persisted throughout the Relevant Period.

200. Brown helped compile the Quarterly Risk review presentations, and received at least two of the 2019 FedRAMP / NIST 800-53 assessments, and received many other documents flagging the repeated failures with regard to (1) the pervasive use of admin rights, (2) the failure to follow the concept of least privilege, and (3) "significant deficiencies" in access

management. These were not isolated instances of an failing to adhere to an access control policy, but systemic, organizational-level failures to employ adequate policies and procedures. Given his knowledge of the systemic, organizational-level failure to employ adequate policies and procedures, Brown knew, or was reckless or negligent in not knowing, that it was a materially false and misleading for him and the Company to claim in the Security Statement that "[a]ccess controls to sensitive data in our databases, systems, and environments are set on a need-to-know / least privilege necessary basis" and "SolarWinds employees are granted a limited set of default permissions to access company resources, such as their email, and the corporate intranet." But those statements remained on the SolarWinds' website throughout the Relevant Period.

b. Brown Ignored Warnings About a Critical Access Management Problem With SolarWinds' Virtual Private Network.

201. In June 2018, Network Engineer D identified a "security gap" or cybersecurity weakness relating to access to SolarWinds' virtual private network or VPN. He documented this in a June 4, 2018 email to multiple people including Senior InfoSec Manager E. The security gap allowed a user with credentials to evade SolarWinds' data loss prevention software by logging on to SolarWinds' VPN network from a device that was not owned or managed by the Company's information technology department. Such unmanaged devices, sometimes referred to as "Bring Your Own Device," often are personal cell phones and laptops that employees use to connect to a company's computer network through a VPN to perform work, including remote work or telework.

202. This VPN security gap was exacerbated by the fact that many SolarWinds employees had administrator rights, allowing them to make changes to security settings, among other things. Additionally, SolarWinds did not follow its existing Enterprise Security Standards

and Guidelines requiring client device integrity checks for the VPN. Such unmanaged devices were not equipped with SolarWinds' data loss prevention software, which would allow the Company to identify and monitor the movement of data within its network and outside its network.

203. Network Engineer D sent an email to various SolarWinds employees, including the Company's Director of IT and Senior InfoSec Manager E, detailing this VPN cybersecurity weakness. In the email, Network Engineer D explained that the configuration was "not very secure for resources currently accessible via VPN and data stored there." Network Engineer D proposed a solution involving the use of "certificates for machine authentication," limiting access to "verified/trusted devices…under IT control," while other users could utilize VPN, but with "access to less resources."

204. After receiving pushback to his initial recommendation and seeing no action to remediate the security gap, on August 24, 2018, Network Engineer D sent a more urgent message seeking to draw attention to the issue. In his message, which he again sent to SolarWinds' Director of Information Technology and Senior InfoSec Manager E, Network Engineer D explained that it was a common practice for users to access SolarWinds' network from unmanaged devices. He explained that, because of the security gap in SolarWinds' VPN, anyone with standard log-in credentials could:

- …access [SolarWinds'] corporate wifi or corporate VPN from ANY device, no matter if [C]ompany owned or not
- While on corporate wifi, or VPN, such device can basically do whatever without us detecting it until it's too late:
    - It can easily download any content without being detected by [SolarWinds' data loss prevention software], which is normally installed on all domain PCs.

- it can compromise entire network by spreading malware (spyware, viruses, trojans, ransomware), because we cannot ensure that such device will be fully compliant in terms of [operating system] updates, antivirus [protection], software installed etc.

205. Network Engineer D highlighted additional concerns in this email, including that (1) SolarWinds should "consider…implementing/deploying new systems without full admin rights"; and (2) "we know that sometimes people are leaving the company, but their [login] cred[entails] remain active for a few more days."

206. On top of his email warnings, Network Engineer D created a presentation describing his concerns ("August 2018 VPN Security Gap Presentation"). He then delivered that presentation on or around August 28, 2018 at a meeting that included managers such as Senior InfoSec Manager E. In the presentation, Network Engineer D explained that in its current state, SolarWinds' VPN ran the risk that an attacker could access and upload code without detection by SolarWinds' data loss prevention software, serve as a backdoor for future attacks, and reside on SolarWinds' network for an extended period without anyone noticing.

207. Among the concerns flagged in the August 2018 VPN Security Gap Presentation, were:

- SolarWinds had "No means to enforce or monitor what devices connect to our network"
- SolarWinds had "No options to guarantee user identity"
- SolarWinds' "[e]mployees do not respect security guidelines [as shown by the fact that they are]
  - installing 3rd party software, even games
  - Using torrents[10]

[10] A torrent is a distributed form of file sharing that is sometimes used to bypass security controls because of its decentralized nature. They are also commonly used to share pirated software or video files.

- The need to "Manage user admin rights" which are "[a]t this time basically unlimited."

208. In particular, the fact the SolarWinds "employees" (plural in the original) were able to, and did, access and use torrents from the SolarWinds network is a major cybersecurity problem, as files downloaded through torrents can include executable program files that conceal malicious code from threat actors.

209. On August 31, 2018, Senior InfoSec Manager E forwarded the June 4, 2018 and August 24, 2018 emails from Network Engineer D and the August 2018 VPN Security Gap Presentation to Brown. Despite the gravity of the concern raised by the network engineer and his expressed view that exploitation of the security gap could lead to significant reputational and financial loss to SolarWinds, Brown failed to elevate the matter further.

210. SolarWinds and Brown failed to take sufficient steps to remediate the VPN security gap in 2018 or 2019. In January 2020, Senior InfoSec Manager E, who had previously forwarded the presentation to Brown, sent it to him again, noting that the recommendation "did not get any traction" when it was raised in 2018.

211. Despite the warnings in August 2018, Brown and others aware of the issue did not take sufficient steps to ensure that this security gap was either fixed or disclosed. No one, including Brown, raised the issue with SolarWinds' Disclosure Committee, nor did SolarWinds have sufficient procedures and controls in place to ensure that he did so. Nor did he, or anyone else at SolarWinds, ensure that SolarWinds enforced its existing internal guidelines requiring client device integrity checks for the VPN.

212. Further, the VPN security gap identified by Network Engineer D was not addressed by compensating or technical controls or other means. Instead, the Company went forward with its October 2018 IPO without (1) disclosing this known security gap, (2) assessing the

materiality of the security gap for disclosure purposes, or even (3) disclosing that it had identified a significant access control issue, thus depriving investors of key information. Nor did the Company take straightforward steps to remedy the security gap to render it immaterial, which would have only required enforcing best practices and using existing, in-place software with little or no cost to block unmanaged devices from accessing SolarWinds' network. The risk of unmanaged devices accessing corporate resources is well-known in the security field, and the Company failed to put even minimal compensating controls in place once the security gap was identified. For example, the Company failed to make any effort to regularly detect or automatically alert the presence of unmanaged devices, and did not undertake an investigation during the Relevant Period to determine whether the security gap had been exploited.

213. The Security Statement remained on SolarWinds' website in its materially false and misleading form, as, again, it never accurately reflected the true state of SolarWinds' access controls, including the VPN issue described above, nor did SolarWinds or Brown otherwise publicly disclose the existence of significant deficiencies in its access controls, including the VPN security gap described by Network Engineer D, which persisted throughout the Relevant Period. Instead, the language quoted above regarding access controls remained on the website throughout the Relevant Period.

c. SolarWinds and Brown's Misstatements and Omissions Regarding Access Controls Were Material.

214. SolarWinds and Brown's false and misleading statements and omissions regarding access controls were not only false and misleading, but materially so. A reasonable investor, considering whether to purchase or sell SolarWinds stock, would have considered it important to know the true state of SolarWinds' security, especially regarding the state of the Company's access controls for its critical "information systems" and "sensitive data." Securities analysts

who followed SolarWinds at the time and issued reports regarding its stock, including Analyst J and Analyst K, confirmed that the expansive, unremediated use of administrator privileges would have been important in determining whether to recommend that investors purchase or sell SolarWinds stock. Indeed, the expansive use of administrator rights is so problematic that it could cause a reasonable analyst to question all of a company's operations.

215. In a presentation for a keynote address by Brown at a security roadshow in August 2018, Brown included information about SolarWinds' own MSP Security Resource Center, and he stressed the importance of practices like "Manag[ing] identities and know[ing] who has access."

216. In a September 2018 webinar that more than 500 people registered to attend regarding "Helping Your Customers Evaluate Risk," Brown discussed that "Identity management done well can greatly decrease the risk faced by a business" and the speaker notes for that presentation included talking points such as "Is access limited to only what people need to do their jobs? Is administrative access controlled and managed?" Brown repeated many of these same points in an episode of his Company-sponsored "Brown Report" podcast around the same time.

217. Additionally, in May 2019, Brown spoke publicly about the importance of access controls in a SolarWinds-sponsored blog post that advised SolarWinds' MSP customers to: "Guard admin privileges with your life: Adhere to the 'principle of least privilege' as much as you can…Users with admin privileges are part of these crown jewels." Brown also stated: "I've always said a well-managed environment is a secure environment. Keeping track of your admin accounts and implementing least privilege can help you mitigate the chances of a ransomware attack launching from a compromised admin account."

218. Additionally, in her January and June 2018 draft performance self-assessments, SolarWinds' CIO identified "Identity and Access Management" and "Security Standards" as two deficiencies that could adversely impact SolarWinds' "IPO ***valuation***."

6. Brown Made Misstatements in Company-Approved Press Releases, Blog Posts, Podcasts, and Presentations.

219. The Security Statement was not the only place where Brown and the Company made materially false and misleading statements related to SolarWinds' cybersecurity practices. Brown acted as SolarWinds' primary cybersecurity spokesperson during the Relevant Period. He highlighted SolarWinds' robust cybersecurity practices in SolarWinds' podcasts, blog posts, press releases, and presentations, while failing to disclose the issues discussed above. Both the blog posts and podcasts were promoted by the Company. And the blog posts were posted on a SolarWinds' website, identified Brown as a SolarWinds employee, discussed his professional background, contained information about SolarWinds' products, and linked to the Trust Center and/or other portions of SolarWinds' website.

220. In a September 2018 presentation to MSP customers titled "Embrace Partnerships to Provide Effective Security" Brown:

a) Stated that "majority of breaches still result from bad cyberhygiene"

b) Instructed that companies need to "Manage identities and know who has access"

c) Asserted that at SolarWinds "We protect our customers and their customers"

d) Warned of the need to evaluate risk and plan accordingly

e) Touted and displayed a screenshot of SolarWinds' Security Resource Center, where SolarWinds' Security Statement was maintained.

221. In a March 2019 podcast referring to SolarWinds' cybersecurity practices, Brown stated that the Company was "focused on…heavy-duty hygiene," which Brown described in sworn testimony as the "things that…make up cyber best practices."

222. Similarly, in a 2020 blog post linked to SolarWinds' website, Brown assured the public that the Company "places a premium on the security of its products and makes sure everything is backed by sound security processes, procedures, and standards." Brown then included a hyperlink in this blogpost to the Trust Center of SolarWinds' website containing the Security Statement, further disseminating the Security Statement. Brown's statement in the blog post that SolarWinds "makes sure everything is backed by sound security processes, procedures and standards" is false because, as discussed above, in truth SolarWinds had multiple unaddressed cybersecurity problems, including its failure to abide by SDL, lack of monitoring, failure to enforce its password policies, and significant deficiencies in access controls.

223. SolarWinds and Brown also promoted the Company's purported commitment to cybersecurity in multiple press releases that were publicly distributed and are maintained on the investor section of the Company's website. This included an October 7, 2019 press release in which SolarWinds stated that the Company "equips technology professionals with tools to help monitor, manage, and secure today's complex IT environments." In that same release, SolarWinds disseminated Brown's statement that "SolarWinds is committed to helping IT and security teams by equipping them with powerful, affordable solutions that are easy to implement and manage. Good security should be within the reach of all organizations."

224. SolarWinds also posted a December 12, 2019 press release to the investor section of its website that touted "SolarWinds' commitment to high security standards, which its partners rely on to help keep the systems they manage secure and compliant." In that same release,

SolarWinds disseminated Brown's statements that SolarWinds and its employees "are always striving to give our partners a leading edge while also fostering a community built on a bedrock of trust," and that meeting security standards "demonstrate[s] a vendor's commitment to privacy and security—something we always strive to improve upon in all we do."

225. These statements were materially false and misleading and contained material omissions. They described SolarWinds' cybersecurity practices to the public in a positive light, touting things such as SolarWinds' purported "commitment to high security standards," and proclaiming the importance of following various cybersecurity practices. Together with the other statements in this Amended Complaint, they sought to create a total mix of information painting a positive public picture of SolarWinds' security practices that is belied by the numerous contemporaneous internal statements and assessments describing SolarWinds' poor cybersecurity practices and policy violations.

7. SolarWinds Had Systemic Cybersecurity Deficiencies.

226. The pervasive cybersecurity issues highlighted above were part of a systemic cybersecurity problem throughout SolarWinds during the Relevant Period and a scheme to conceal these issues from investors and customers.

227. For example, in October 2018, the same month as SolarWinds' IPO, Brown sent a presentation to SolarWinds' CIO that warned (again) that:

- SolarWinds needed to "Lock down our critical assets that could cause a major event";
- the "[c]urrent state of security leaves us in a very vulnerable state for our critical assets"; and
- "[a] compromise of these assets would damage our reputation and financially [sic]."

The presentation also included multiple red text warnings such as "Many independent user stores still in use and not well controlled." And the presentation flagged the risk that "[l]ack of cyber

hygiene leaves us open to being a target of opportunity." As discussed below, despite this frank recognition of SolarWinds' multi-faceted and significant cybersecurity problems and risks, the Company made no effort to adequately disclose the true state of its cybersecurity in disclosures to investors, including in connection with the IPO, which instead only included generic warnings. Many of the issues in this presentation had been flagged as problems as far back as August or September 2017. But, despite repeated warnings, SolarWinds did not fix these issues in the year-plus that passed from the first warnings to the IPO, or disclose them to investors.

228. As another example, Security & Compliance Manager L warned in an April 15, 2020 email to Brown that even the group that reported to the CIO was not incorporating cybersecurity practices into their work. She warned that "we have a ***systemic issue*** around lack of awareness for Security/Compliance requirements with most if not all [of the information technology group's] projects" and cybersecurity "requirements [are] not thought of or ingested upfront, the result is a complete scramble and process piecemeal either right before or after, a system is live."

229. Similarly, in instant messages sent in November 2020, Senior InfoSec Manager E expressed his own disgust with the Company's cybersecurity posture: "[W]e're so far from being a security minded company. [E]very time I hear about our head geeks talking about security I want to throw up."

230. Indeed, the poor state of SolarWinds' cybersecurity posture seemed to be a joke for employees in its InfoSec group, at least prior to the SUNBURST hack being revealed. In November 2020, InfoSec Employee F and Senior InfoSec Manager E exchanged the following messages before Senior InfoSec Manager E's vacation:

F: …I hope you have a good time off and I will try to man the fort!

E: more like keep the house from burning down! Lol

F: hard with all these faulty electrics

231. Brown was not only aware that SolarWinds had systemic cybersecurity problems, but he also presciently appeared to warn that actions like this SEC enforcement case would be needed before companies took cybersecurity seriously. In a February 2019 email he revised and approved a quote that a SolarWinds press spokesperson sent to a reporter writing a cybersecurity article. The quote said "training and education" were "the best way to influence behavior" regarding cybersecurity. But in that same email chain, Brown candidly admitted that "In reality I believe that the best way to improve global cyber security is with legislation and penalties."

232. As described above, by virtue of all of the internal communications and documents laying out the systemic, longstanding cybersecurity failures at SolarWinds, SolarWinds and Brown knew, or were reckless or negligent in not knowing, that the listed statements in the Security Statement, podcasts, and blogs contained materially false and misleading statements, and that SolarWinds and Brown had omitted and failed to disclose (either in the Security Statement or in other public statements) the true state of SolarWinds' cybersecurity practices, including the risks, issues, and violations discussed in this Amended Complaint. Those omissions made those statements, in light of the circumstances, materially misleading.

233. The materiality of many of the issues described above is heightened by the presence of many of the other issues. For example, the materiality of SolarWinds having both the VPN issue and the pervasive use of admin rights is greater than either issue alone. This is not a case about a single control failure or a handful of isolated control failures. Rather, the widespread and persistent failure to follow each of the policies outlined above (following the NIST Cybersecurity Framework, utilizing an SDL, network monitoring, password management, and

access controls) was material. And even if the persistent failure to follow one of those policies was not material, collectively the persistent failure to follow them all was material.

234. Working together, the false statements in the Security Statement and elsewhere wove a false and misleading narrative that concealed deep-seated security issues that presented immediate business risks by imperiling sales and damaging customer relationships and also exposed SolarWinds to significant reputational harm, costly legal liability, and other major risks that were material to investors.

235. The flaws described above, at least when viewed in their totality across multiple years, are not mere imperfections, or the minor deviations from practices that a company might normally experience. Rather, they represent systemic, longstanding problems which rendered the Security Statement materially false and misleading and significantly increased the risk of material cyberattack. A company cannot choose to tout that it does "penetration testing" and follows the concept of "least privilege" and then claim that acknowledging it routinely fails to do either would give hackers too much of roadmap.[11]

236. Brown was the maker of the statements described above for the reasons described above, and his knowledge, recklessness, and/or negligence imputes to the Company for the reasons described above and by virtue of his role as an officer of SolarWinds, head of its InfoSec group, chief spokesperson on cybersecurity issues, and the literal "face" of cybersecurity at the Company (his picture was prominently displayed on the "Trust Center" of SolarWinds' website where the Company posted the Security Statement).

[11] The SEC is not asserting that SolarWinds needed to follow the SEC's 2023 Final Rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, or attempting by this litigation to impose more specific requirements than that rule imposes. *See* https://www.sec.gov/files/rules/final/2023/33-11216.pdf

237. Additionally and alternatively, the SolarWinds employees involved in and responsible for these issues, including those described above, collectively knew, or were recklessness or negligent in not knowing, that the Security Statement was false and misleading and contained misleading material omissions for the reasons described above.

238. Finally, given all of SolarWinds' cybersecurity problems discussed above, Brown and other SolarWinds executives could have reasonably anticipated that SolarWinds would be subject to a material cyberattack.

D. SolarWinds Made Materially False and Misleading Statements About Its Cybersecurity Practices in Its SEC Filings.

239. SolarWinds returned to being a publicly traded company through a (second) Initial Public Offering registered via a Form S-1 that was filed with the SEC on October 18, 2018, and which was signed by the Company's CEO and CFO. This registration statement contained a boilerplate disclosure regarding cybersecurity risks.

240. SolarWinds' sole cybersecurity risk disclosure in its October 2018 Registration Statement on Form S-1 provided that:

> **If we sustain system failures, cyberattacks against our systems or against our products, or other data security incidents or breaches, we could suffer a loss of revenue and increased costs, exposure to significant liability, reputational harm and other serious negative consequences.**
>
> We are heavily dependent on our technology infrastructure to sell our products and operate our business, and our customers rely on our technology to help manage their own IT infrastructure. Our systems and those of our third-party service providers are vulnerable to damage or interruption from natural disasters, fire, power loss, telecommunication failures, traditional computer "hackers," malicious code (such as viruses and worms), employee theft or misuse, and denial-of-service attacks, as well as sophisticated nation-state and nation-state-supported actors (including advanced persistent threat intrusions). The risk of a security breach or disruption, particularly through cyberattacks or cyber intrusion, including by computer hacks, foreign governments, and cyber terrorists, has generally increased the number, intensity and sophistication of attempted attacks, and intrusions from around the world have increased. In addition, sophisticated hardware and operating system software and applications that we procure from

> third parties may contain defects in design or manufacture, including "bugs" and other problems that could unexpectedly interfere with the operation of our systems.
>
> Because the techniques used to obtain unauthorized access or to sabotage systems change frequently and generally are not identified until they are launched against a target, we may be unable to anticipate these techniques or to implement adequate preventative measures. We may also experience security breaches that may remain undetected for an extended period and, therefore, have a greater impact on the products we offer, the proprietary data contained therein, and ultimately on our business.
>
> The foregoing security problems could result in, among other consequences, damage to our own systems or our customers' IT infrastructure or the loss or theft of our customers' proprietary or other sensitive information. The costs to us to eliminate or address the foregoing security problems and security vulnerabilities before or after a cyber incident could be significant. Our remediation efforts may not be successful and could result in interruptions, delays or cessation of service and loss of existing or potential customers that may impede sales of our products or other critical functions. We could lose existing or potential customers in connection with any actual or perceived security vulnerabilities in our websites or our products.

(emphasis in original)

241. This disclosure recited generic harms that could befall SolarWinds and that most companies—especially in the IT industry—face on an ongoing basis. But it did nothing to alert investors to the elevated risks that existed at, and were specific to, SolarWinds because of its poor cybersecurity practices. Those risks are not being assessed in hindsight by the SEC. Brown and others at SolarWinds assessed and documented them at the time. Indeed, during the very month that SolarWinds made the above public disclosure, Brown stated (internally) that the "current state of security leaves us in a very vulnerable state for our critical assets."

242. Brown was one of the people responsible for the technical content and accuracy of this risk disclosure. During the SEC's investigation, Brown testified that while he did not review the precise disclosure language SolarWinds used in its SEC filings, he was asked factual questions, reviewed documentation, and provided information that he understood that

SolarWinds' legal team and others used to create risk disclosures in its SEC filings. This was confirmed at a high level by SolarWinds, who represented to the SEC, through counsel, that "[m]embers of the Company's legal team consulted with individuals from the Company's CIO department in connection with drafting the cyber risk factors" in the Form S-1. Brown reported directly to the CIO and was part of her department.

243. SolarWinds' disclosures failed to convey the known risks discussed above, or even that known risks of this type had been identified. Even if some of the individual risks and incidents discussed in this Amended Complaint may not each have risen to the level of requiring disclosure on their own, at least collectively they created such an increased risk to SolarWinds that the failure to disclose their collective impact on SolarWinds' cybersecurity posture rendered the risk disclosures that SolarWinds made materially misleading.

244. Despite internally documenting all the cybersecurity issues and problems discussed above, and despite multiple internal warnings about their severity, SolarWinds neither specifically disclosed the issues nor generally disclosed that known, unremediated issues with NIST Cybersecurity Framework compliance, SDL, network monitoring, access controls (including the VPN security gap), or passwords existed. Nor did SolarWinds even disclose Brown's assessment that its "critical assets" were "very vulnerable." Investors considering purchasing shares in connection with SolarWinds' IPO had a right to know—and would have considered it important to know—the Company's serious internal concerns and deficiencies surrounding access and privilege to the Company's critical assets and data. As a result, SolarWinds' October 18, 2018 Form S-1—and particularly the risk disclosure quoted above—was materially misleading.

245. Brown and SolarWinds made public statements about SolarWinds' cybersecurity, including numerous statements casting its cybersecurity practices in a positive light. Assessing the total mix of information SolarWinds chose to make public on the topic of cybersecurity, it was materially false and misleading for SolarWinds to make those statements, without, at a minimum, disclosing at roughly comparable level of technical detail that it had systemic cybersecurity failures. Indeed, SolarWinds and Brown specifically claimed in public statements that the Company followed important cybersecurity practices that they knew the Company did not follow.

246. SolarWinds' risk disclosure was inadequate because the numerous, systemic, material, longstanding problems with its cybersecurity practices, and known and increasing incidents and risks, so increased its risk profile that merely disclosing that it faced the same risk of cyberattacks (and natural disasters, fires, etc.) that any company in the technology sector faced was inadequate, because the truth was that its poor cybersecurity practices placed it at materially increased risk.

247. Brown and SolarWinds knew, or were reckless or negligent in not knowing, about the numerous cybersecurity risks and problems, but nonetheless SolarWinds decided to conduct an IPO without first remediating those problems to render them immaterial.

248. The SEC issued guidance on this topic well before SolarWinds conducted its IPO, underscoring in the February 26, 2018 Final Rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure:

> Given the frequency, magnitude and cost of cybersecurity incidents, the Commission believes that it is critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion, ***including those companies that are subject to material cybersecurity risks but may not yet have been the target of a cyber-attack.*** (emphasis added).

249. Here, SolarWinds and Brown, even prior to the SUNBURST attack, materially misled the market and investing public by putting forth a total mix of information, including the risk disclosures, the Security Statement, and the other statements quoted above that painted a materially misleading picture of the risks faced by SolarWinds due to its systemic, documented failure to follow the cybersecurity practices it publicly claimed to follow.

250. Risk factors, and changes to risk factors, in a company's SEC filings are commonly reviewed by investors and securities analysts in connection with decisions and recommendations to purchase or sell stock. A reasonable investor, considering whether to purchase or sell SolarWinds stock, would have considered it important to know the true nature and scale of the cybersecurity risks specifically facing SolarWinds, not merely generic risk disclosures that companies typically might face and which did not accurately reflect the known significance of SolarWinds' risks. A reasonable investor would have also wanted to know about the Company's known and increasing risk of cyberattacks, which could have materially negative effects on the Company, and which were not adequately conveyed through the Company's generic disclosure. Additionally, as discussed above (in paragraph 103), for SolarWinds, increased risk of a cybersecurity event had particular significance. SolarWinds' misleading Form S-1 deprived investors of that material information.

251. SolarWinds then repeated (or incorporated by reference) the exact same materially misleading risk disclosures, in the following SEC filings throughout the Relevant Period:

Filing Type	**Date Filed with SEC**
Form 10-Q, Quarterly Report	November 27, 2018
Form 10-K, Annual Report	February 25, 2019
Form S-8, Registration Statement	April 11, 2019
Form 10-Q, Quarterly Report	May 10, 2019
Form S-1, Registration Statement	May 20, 2019
Form 10-Q, Quarterly Report	August 12, 2019
Form 10-Q, Quarterly Report	November 7, 2019

Filing Type	Date Filed with SEC
Form S-8, Registration Statement	December 11, 2019
Form 10-K, Annual Report	February 24, 2020
Form S-8, Registration Statement	February 24, 2020
Form 10-Q, Quarterly Report	May 8, 2020
Form 10-Q, Quarterly Report	August 10, 2020
Form 10-Q, Quarterly Report	November 5, 2020

252. Worse still, SolarWinds made these repeated misleading disclosures even as an accumulating number of red flags piled up throughout 2020. In other words, this generic warning was materially false and misleading when first made and only became worse over time. The Company's failure to disclose the accumulating red flags left investors without sufficient warning that there had been multiple successful intrusions against Orion, as discussed above, or that SolarWinds' overall cybersecurity posture was so poor that something far worse could be just around the corner.

253. SolarWinds also failed to remediate the issues described above ahead of its IPO in October 2018, and for many of them, for months or years afterwards. Thus, threat actors were able to later exploit the known, ***still unremediated*** VPN security gap to access SolarWinds' internal systems in January 2019, avoid detection for nearly two years, and ultimately insert malicious code resulting in the SUNBURST cyberattack.

E. SolarWinds and Brown Failed to Disclose Red Flags and Warning Signs of a Cyberattack Leading up to the Revelation of the SUNBURST Cyberattack.

1. In January 2019 Threat Actors Accessed SolarWinds' Network Environment via VPN Using an Unmanaged Device.

254. In January 2019, just months after SolarWinds' IPO, the threat actors responsible for the SUNBURST cyberattack accessed SolarWinds' corporate VPN by using an unmanaged third-party device and stolen credentials, exploiting the VPN cybersecurity weakness that Network Engineer D had identified six months earlier. During those six months, SolarWinds and Brown had neither remediated nor disclosed this weakness.

255. From approximately January 2019 through approximately November 2020, the threat actors repeatedly accessed SolarWinds' network through a VPN. During that time, the threat actors conducted reconnaissance, exfiltration, and data collection; identified product and network vulnerabilities; harvested credentials of SolarWinds employees and customers; and planned additional attacks against SolarWinds' products that would be deployed during later stages of the campaign.

256. As anticipated in Network Engineer D's August 2018 presentation, once the threat actors accessed the system through a VPN connection on an unmanaged device, they were able to access SolarWinds' entire network, moving laterally between its corporate and software development zones. In part due to access control deficiencies described above, the threat actors were able to elevate privileges, disable antivirus software, and access and exfiltrate data, including computer code and customer information, without triggering alerts from SolarWinds' data loss prevention software. The threat actors used multiple accounts that had administrator privileges, exploiting a security problem that SolarWinds had known about since at least June 2017. The threat actors were also able to access and monitor network access and emails of SolarWinds' key personnel without detection. This included exfiltrating approximately 7 million emails from more than 70 SolarWinds employees between approximately December 2019 and December 2020, including emails from employees in the Information Technology and Security groups.

257. Following months of reconnaissance and data exfiltration from the SolarWinds' networks, in November 2019, the threat actors used information gained from their access to SolarWinds' networks and data to begin a trial run of what ultimately became the SUNBURST attack. The threat actors conducted this trial run by first inserting non-malicious test code into

SolarWinds' Orion software builds to determine whether they could successfully evade detection.

258. Seeing that their insertion of non-malicious code went undetected, in February 2020, the threat actors began inserting malicious code into Orion software builds. Over the next several months, the threat actors inserted malicious code into three different Orion software builds that went out to nearly 18,000 customers. The impacted customers included numerous federal and state government agencies, and more than 1,500 publicly traded U.S. companies, banks, broker-dealers, accounting firms, and other entities regulated by the SEC. The malicious code provided the threat actors a backdoor into the network environments of SolarWinds' customers who downloaded and installed the infected versions of the software to systems that were connected to the internet. The threat actors utilized the SUNBURST attack to conduct additional secondary attacks on approximately 100 of the 18,000 impacted companies and government agencies.

259. In certain reports, the SUNBURST attack has been attributed to a nation-state actor. But the vulnerabilities that the threat actors exploited to access SolarWinds' system and ultimately infect its customers' systems were vulnerabilities that SolarWinds and Brown had known about for months and that could have been remedied through straightforward steps. The possibility that SUNBURST was committed by a nation-state actor neither excuses SolarWinds' failure to adhere to ***basic*** cybersecurity practices, nor justifies the Company hiding those failures from the investing public.

2. Throughout 2020, SolarWinds and Brown Learned of Focused Attacks on Its Orion Products and Other Platforms.

260. Beginning in early 2020, SolarWinds and Brown learned of an increase in threats to its products and customers, including multiple attacks against customers' Orion platforms. In

addition, the Company and Brown learned of multiple serious vulnerabilities in the Orion platform products. The additional risks, attacks, and vulnerabilities served as red flags indicating that SolarWinds had been, or was at increased risk of soon becoming, the victim of a significant cyberattack. None of these red flags were disclosed during the Relevant Period, either in the Company's periodic filings or otherwise.

a. SolarWinds Learned of Multiple Attacks Against Its MSP Platforms During 2020.

261. As discussed (in paragraph 197), SolarWinds was aware of multiple access control problems around the MSP portal. Perhaps unsurprisingly given the security problems, in the first half of 2020, at least nine MSPs who were SolarWinds customers suffered attacks through SolarWinds' MSP products, including ransomware attacks. All nine of the attacks involved the use of accurate credentials on the threat actors' first attempt, suggesting that the threat actors had somehow obtained the credentials before the attacks. The attacks led SolarWinds to investigate whether its database of customer credentials may have been compromised, a concern that SolarWinds was unable to resolve and a red flag that its own systems may have been compromised.

262. In March 2020, SolarWinds learned that a threat actor had attacked SolarWinds' MSPs using a list of 19,000 single sign-on customers, meaning that the threat actors had information to distinguish between customers who had enabled more secure multi-factor authentication and customers who did not have it enabled. Despite investigation, SolarWinds was unable to identify where the threat actors obtained the list of 19,000 single sign-on customers. This was another red flag that malicious actors had access to SolarWinds' network and/or systems.

263. In both cases, SolarWinds failed to determine how the threat actors had obtained the credentials or list of single sign-on customers, though Company personnel, including Senior InfoSec Manager E, theorized that it might have been through a breach of SolarWinds' systems.

264. In June 2020, Brown acknowledged the ongoing problems with the Company's MSP products, including that the threat actors exhibited a high degree of familiarity with the Company's MSP products. This indicated that the threat actors had likely conducted reconnaissance on, and were specifically targeting, SolarWinds' MSP products and customers. Brown also provided SolarWinds' CIO and CTO at least partial updates regarding these issues, including information evidencing the threat actor's high level of familiarity with the MSP products. In a July 2020 presentation to product managers in SolarWinds' MSP business unit, Brown stated that the threat actors "know N-Central [SolarWinds' MSP product]…Know how to deploy software, shut off backup etc." The threat actors' ability to "deploy software, shut off backup" was another red flag.

265. But none of the MSP issues, or Brown's assessment of them, was disclosed to investors during the Relevant Period, either by (a) specifically listing the issues, (b) disclosing a general statement that alerted investors that SolarWinds was facing increased cybersecurity issues that signified a potential focused attack on, and compromise to, their systems, or (c) any other form.

266. These attacks on SolarWinds' MSPs were material. As Brown acknowledged, like Orion, the MSP products were among the Company's "crown jewels" that needed to be protected. In a September 2019 interview, Brown stated:

> So, as part of our crown jewels, our MSP business is absolutely, 100-percent at the top of my risk level. They are my risk level, because I realize what access we grant to them. So if you look across my assets at SolarWinds, that is absolutely one of the major crown jewels I watch very closely. Our board watches very

closely. That's what we get questions about from our risk committee and others, is 'Do we have enough protection around the MSP environment?'

3. SolarWinds and Brown Learned of Attacks on, and Vulnerabilities in, Its Orion Products in 2020.

267. Several times before December 2020, customers alerted SolarWinds to evidence that threat actors were not only specifically targeting SolarWinds' Orion platform and customers, but had breached SolarWinds' systems. U.S. Government Agency A and Cybersecurity Firm B notified SolarWinds of incidents that took place in May and October 2020, respectively, that were later linked to the SUNBURST cyberattack. SolarWinds did not publicly disclose any of these incidents (either individually or through their collective impact), update the Company's overall risk disclosure in any way, or identify and remediate the vulnerabilities to render them immaterial.

a. The May 2020 Attack on U.S. Government Agency A Reveals Too Many Vulnerabilities for SolarWinds to Handle.

268. In 2020, U.S. Government Agency A evaluated and installed SolarWinds' Orion software on a trial basis to determine whether it wanted to purchase the software. During that evaluation process, and before the attack described below, a member of SolarWinds' sales team misrepresented to U.S. Government Agency A that SolarWinds was compliant with FedRAMP, the federal government-wide compliance program for which SolarWinds had more than 60% of the controls lacking—while knowing, or recklessly or negligently not knowing, that the Company was not compliant—as part of the effort to convince U.S. Government Agency A to purchase and use the Orion platform.

269. In June 2020, U.S. Government Agency A notified SolarWinds about malicious activity by the Orion software after it had been installed on a trial basis by the agency in May 2020. U.S. Government Agency A informed SolarWinds that, during the trial, the Orion software

reached out to contact websites with an unknown purpose and asked the Company to investigate. SolarWinds determined that the portion of the Orion software known as the BusinessLayer was what was causing the software to reach out and that when reaching out, the software was attempting to provide information to the website about the network on which it was located. Additionally, SolarWinds uncovered evidence that the threat actors who were attacking U.S. Government Agency A had conducted reconnaissance on the Orion platform since at least mid-2019 and were mimicking SolarWinds' communication protocols to obfuscate the malicious activity.

270. Brown was aware of the May 2020 attack against U.S. Government Agency A by June 2020. Despite the potential severity of this issue, SolarWinds' internal investigation failed to uncover the root cause for the malicious activity or otherwise remediate the vulnerability in the widely used Orion software. SolarWinds' inability to determine the root cause for this attack was another red flag.

271. A June 18, 2020 instant message conversation among several employees, including InfoSec Employee F, recognized the potential that the U.S. Government Agency A attack could be an ongoing attack against multiple customers:

> Employee: …are you aware of any other incident like this where it seems that Orion was used for attack? My biggest concern is that we have exploit somewhere and there are other cases like this but unnoticed.
>
> F: No.…That's my concern too.

272. In a subsequent July 1, 2020 email to Brown, a member of the Engineering team described being "spooked" by Orion's activity at U.S. Government Agency A. Brown determined that there were only two possible scenarios: (1) the attacker was already present on the customer's system or (2) the attackers were looking closely at Orion "for methods to utilize it in larger attacks." Brown asserted that the incident was "very concerning" and continued, "[a]s

you guys know our backends are not that resilient and we should definitely make them better." At no point during the Relevant Period did Brown or SolarWinds disclose Brown's assessment that portions of SolarWinds' information technology structure were "not that resilient" or that the attack was "very concerning" due in part to possibility that SolarWinds' systems were compromised.

273. Brown did not ensure that the U.S. Government Agency A attack was properly treated under SolarWinds' Incident Response Plan. That plan scored incidents on a scale from 0 / Minimal to 3 / High. Incidents scored 2 or higher required notification to SolarWinds' CEO, CTO, and others. An incident should have been scored 2 or higher when it "[i]nvolves a security compromise that affects multiple customers, whose impact could have an adverse effect on SolarWinds' reputation, revenue, customer(s), partner(s) or the public (I.e. Remote Code Execution)" and this "[i]ncludes a report of compromise for which other customers are susceptible."

274. For the U.S. Government Agency A attack, Brown flagged that it could be part of a "larger attack[]" campaign involving SolarWinds' flagship product that could affect more SolarWinds customers. Plus SolarWinds was unable to determine the source of the attack and rule out this possibility. The attack was nonetheless scored as a 0 / minimal incident, and Brown did not inform the CEO about the attack.

275. In testimony during the SEC investigation, Brown described the attack on U.S. Government Agency A as "unique" explaining that "this was – and somewhere in here I'm sure you see that this was a unique instance. This was a concerning incident because what our belief was is that – so the OIP server that's talked about is our internally-hosted server, right? That's what OIP is. It's not – it's something inside our environment." Brown elaborated that "[w]hat

was the unique component of DOJ which got us concerned is that the traffic going to that environment looked like a piece of, you know, additional software that was installed on the machine that was targeting SolarWinds" and that "it was very unique to that environment because we had never seen anything like this before."

276. The Company's internal investigation of the attack uncovered "numerous" vulnerabilities—some of which had been present and identifiable for years—that needed to be remedied to protect the Orion platform from future attacks. The large increase in incidents and vulnerabilities led SolarWinds' employees to complain to Brown and other InfoSec employees that they were inadequately staffed to address the large number of vulnerabilities being identified in June and July 2020, and that fixing all of the issues—even with adequate staff—would take years.

277. SolarWinds used Risk Acceptance Forms to document instances where risks fell outside SolarWinds' "standard guidelines," regarding cybersecurity. Brown was one of the small group of people authorized by the Company to accept and approve such risks, and generally was one of the two people who would approve them. In September 2020, a manager from SolarWinds' engineering team submitted for approval a Risk Acceptance Form that went to Brown and others. The form asked them to "accept[] the risk of legacy issues in the Orion Platform" because "[t]he volume of security issues being identified over the last month have outstripped the capacity of Engineering teams to resolve."

278. Despite having and using Risk Acceptance Forms to document risks, during the Relevant Period, SolarWinds does not appear to have had a related process for the Company to determine if there were too many flaws or risks in a product and that a product should no longer be distributed to customers.

b. The October 2020 Attack on Cybersecurity Firm B Prompts SolarWinds to Lie to Conceal Orion's Flaws.

279. In October 2020, another SolarWinds customer, Cybersecurity Firm B, notified the Company about malicious activity by Orion software, which included the BusinessLayer reaching out to a website and downloading a malicious file. SolarWinds' employees at the time recognized and discussed internally that the activity was similar to the activity reported a few months earlier by U.S. Government Agency A. Individuals in SolarWinds' InfoSec team recognized the unique nature of the intrusion and noted that both attacks utilized SolarWinds' BusinessLayer to reach out to external websites that it should not have been contacting in the ordinary course of operations.

280. In October 2020, Brown was informed of the Cybersecurity Firm B incident and the similarities between it and the May 2020 U.S. Government Agency A incident. An email on October 14, 2020 that was later forwarded to Brown on October 16, 2020 says in part "[Cybersecurity Firm B] in touch with customer support and it seems they had a breach similar to [U.S. Government Agency A]. This does not appear to be OIP (that we know of yet) related, but the business layer was used in the attack chain according to them. In this case however it was to do [BusinessLayer] running some malicious download." This was another red flag, especially because it strongly indicated that of the two possible scenarios Brown outlined after the attack on U.S. Government Agency A, the reality was that SolarWinds' systems were compromised. In other words, by October 2020 if not earlier, SolarWinds and Brown knew, or were reckless or negligent in not knowing, that the Company's systems had been breached.

281. In a November 5, 2020 group instant message conversation involving more than a dozen SolarWinds employees, multiple different employees recognized the similarities between

the U.S. Government Agency A attack (which Brown described as "unique") and the Cybersecurity Firm B attack, saying things like:

- "seems similar to [U.S. Government Agency A] where BusinessLayer was also used to attack";
- "We had similar case with [U.S. Government Agency A]. BL [BusinessLayer] was used during an attack";
- "[InfoSec Employee F] was driving the [U.S. Government Agency A] [response], can we got him on this one as well?"; and
- "I'm curios [sic] what happened on [U.S. Government Agency A] and this could be a way to find out."

282. SolarWinds InfoSec staff had multiple communications with Cybersecurity Firm B regarding this attack. In that same November 5, 2020 group instant message, the question was raised whether to alert Cybersecurity Firm B that there had been a prior attack through the BusinessLayer. InfoSec Employee F responded "Id [sic] prefer nobody says on the call that we have seen something like this in the past." InfoSec Employee F then separately messaged Senior InfoSec Manager E, who confirmed that they should not disclose the prior attack to Cybersecurity Firm B.

283. Later that day, during a telephone call with SolarWinds InfoSec employees, personnel from Cybersecurity Firm B asked if SolarWinds had ever seen Orion act as it had during the attack. In truth, as InfoSec Employee F and others at SolarWinds knew, Orion had acted the same way during the U.S. Government Agency A attack. Nonetheless, in accordance with Senior InfoSec Manager E's guidance, InfoSec Employee F falsely informed Cybersecurity Firm B that they had not previously seen similar activity from the Orion platform. In contemporaneous instant messages sent during the telephone call with the customer, InfoSec Employee F messaged his colleague, "***Well I just lied***." Then, despite recognizing the similarities with the earlier incident, InfoSec employees instead informed Cybersecurity Firm B that they

believed the activity was linked to a different, known issue because Cybersecurity Firm B had not applied a previous patch.

284. After the call, Cybersecurity Firm B emailed SolarWinds stating that it appeared to be an "unknown vulnerability" at play, rather than what SolarWinds had suggested, and strongly encouraging SolarWinds to handle the incident as "an external attacker." Despite repeated requests from the customer for assistance, SolarWinds again failed to investigate sufficiently, uncover the root cause for the malicious activity, or otherwise remediate the vulnerability in the Orion software, which was being used by thousands of customers worldwide.

285. SolarWinds and Brown knew, or were reckless or negligent in not knowing, that the similar attacks on U.S. Government Agency A and Cybersecurity Firm B, both through the Orion BusinessLayer, suggested a problem with the Orion software and a compromise in SolarWinds systems. Nonetheless, even after the Cybersecurity Firm B attack, SolarWinds and Brown did not disclose to investors any warning about this situation affecting its flagship Orion product, which accounted for 45% of SolarWinds revenue; nor did they determine the source of the potential problem and remediate it.

286. As discussed above, following the U.S. Government Agency A attack, Brown assessed that there were two possibilities: either (1) the attacker was already at U.S. Government Agency A, or (2) someone was looking to use Orion in larger attacks. After the Cybersecurity Firm B attack, Brown knew, or was reckless or negligent in not knowing, that an attack was almost surely looking to use Orion in a larger attack. Nonetheless, despite all the warning signs discussed above, Brown still failed to sufficiently elevate these attacks within SolarWinds, and SolarWinds failed to disclose to investors its knowledge of the increasing cybersecurity risks that were directly impacting its products and customers.

287. Brown did not ensure that the Cybersecurity Firm B attack was treated properly under the SolarWinds' Incident Response Plan. Instead, like the U.S. Government Agency A attack, the Cybersecurity Firm B attack was rated as 0 / minimal on SolarWinds' incident response plan, because—despite Brown and multiple other SolarWinds employees recognizing the connection to the U.S. Government Agency A attack—it was treated as only affecting a single customer. As discussed above, incidents affecting multiple customers should have been scored as "2" or higher, and elevated to the CEO and CTO in part to determine if they needed to be disclosed to the investing public. Brown failed to ensure that the CEO and CTO knew of the Cybersecurity Firm B attack.

288. Thus, even if SolarWinds' Incident Response Plan called for incidents potentially affecting more than one customer to be treated as level "2" and elevated to the CEO and CTO for disclosure evaluation, employees (including Brown) did not follow that disclosure policy, either knowingly, recklessly, or negligently.

289. The information that SolarWinds' Orion product had been utilized in two linked attacks in 2020 was material information that SolarWinds failed to disclose to investors. Investing Entity I purchased a large quantity of SolarWinds stock in December 2020, after the U.S. Government Agency A and Cybersecurity Firm B incidents had taken place and been linked by SolarWinds employees, but before they had been disclosed. A senior representative from Investing Entity I who led the team responsible for Investing Entity I's decision to purchase SolarWinds stock confirmed to SEC staff that, if there were two attacks against SolarWinds' Orion product in 2020 that SolarWinds employees had determined were linked, that representative would have wanted to know about that information, and have had the opportunity

to ask more questions about the nature of those attacks, before deciding whether to go forward with the investment.

4. Brown and Others Knew About the Extensive Risks to SolarWinds' Orion Products.

290. Brown was aware of the extensive risks and vulnerabilities to SolarWinds' Orion platform and other products, as shown by multiple internal documents.

291. A July 2020 presentation to SolarWinds Product Management group (prepared by Brown and reviewed by SolarWinds' CIO and SolarWinds' CTO) admitted that "SolarWinds [was] no longer under the radar." The presentation described "[Distributed Denial of Service] attacks against marketing sites," "targeted attacks against products," and "sophisticated phishing attacks increasing." It also warned that "[r]econ [was] conducted as early as mid-2019 against SWI" and that Solar Winds' "[i]nternal investigation [had] uncovered additional risks with OIP [the Orion Improvement Program] as an overall service." And the presentation pointed to evidence of reconnaissance against the Company's MSP products, noting that the MSP attackers "know N-Central [the MSP product]. Know how to deploy software, shut off backup etc…"

292. In a July 1, 2020 email to members of SolarWinds' engineering department, Brown wrote:

> We have been getting hit by a lot of activity in the last couple of months. Targeted DDOS attacks against our Websites, Bot nets flooding us with failed login attempts first to Take Control UI and then to Take Control API, multiple account takeovers for MSP admins of N-Central. We are definitely not flying under the radar, because of this ***I'm thinking that some threat groups may also be looking at Orion.***

293. An October 2020 presentation that Brown helped prepare gave a similar description, noting that SolarWinds was no longer under the radar, that threat actors had specifically targeted SolarWinds' products, and that threat actors had been conducting reconnaissance against SolarWinds' products since mid-2019.

294. During October and November 2020, SolarWinds was informed of at least eight other high-risk vulnerabilities affecting the Orion platform through the Zero Day Initiative, a program that rewards security researchers for privately reporting vulnerabilities. The Zero Day Initiative vulnerabilities included remote code execution vulnerabilities, which Brown described as "the most serious" form of vulnerabilities. SolarWinds never disclosed these vulnerabilities during the Relevant Period.

295. An October 2020 Quarterly Risk Review presentation sent to Brown and others highlighted what Brown had said previously: "Events show that [SolarWinds'] products have [been] explicitly targeted" and that "[t]hreat actors have invested time and have done research and modeling of our products prior to executing attacks."

296. In November 2020, an InfoSec employee sent an instant message to Senior InfoSec Manager E with a link to a list of more than a dozen high risk vulnerabilities in the Orion platform stating, "The products are riddled and obviously have been for many years." The next month, a SolarWinds network engineer complained, "We filed more vulnerabilities than we fixed. And by fixed, it often means just a temporary fix…but the problem is still there and it's huge. I have no idea what we can do about it. Even if we started to hire like crazy, which we will most likely not, it will still take years. Can't really figure out how to unf**k this situation. Not good." Undersized staff to respond to cybersecurity incidents was not a new complaint—SolarWinds' CIO had identified it to SolarWinds' CEO as a "key risk" in 2019. The backlog and inadequate staffing were additional red flags. None of the backlog or staffing issues were disclosed to the investing public during the Relevant Period.

297. Thus, in contrast to October 2018, when Brown assessed that while SolarWinds' "critical assets" were "very vulnerable," but there were "[n]o current signs of being a focus of

targeted threats. Currently [we are only] a target of opportunity," Brown and SolarWinds knew, by November 2020, that the Company, and its flagship Orion product specifically, were the focus of far more targeted attacks, including some that had been successful. None of these risk factors affecting "crown jewel" products were disclosed to the investing public during the Relevant Period, either specifically or through an overall disclosure that alerted investors that SolarWinds was experiencing increased indications that its products had been successfully compromised by threat actors. Rather, SolarWinds repeated the same misleading, generic risk disclosures in filing after filing while red flags piled up around the Company and critical, known cybersecurity problems went unremediated for years.

5. Despite Increasing Warnings, SolarWinds Repeated Its Same Materially False and Misleading Risk Disclosures in SEC Filings.

298. At no point between the time of its IPO in October 2018 and the disclosure of SUNBURST in 2020 did SolarWinds disclose the numerous risks, vulnerabilities, and incidents affecting its products in its SEC filings or elsewhere. Instead, in each periodic disclosure and registration statement during the period, SolarWinds disclosed the same hypothetical, generalized, and boilerplate description that had appeared in its October 2018 Form S-1. SolarWinds had experienced events, attacks, and red flags prior to and throughout 2020. As described above, Brown knew, or was reckless or negligent in not knowing, that SolarWinds' critical assets were vulnerable, that SolarWinds was not following important cybersecurity policies, and that it had been the subject of attacks. Nonetheless, Brown signed sub-certifications relied on by the senior executives responsible for signing and certifying the filings that contained the disclosures, confirming that all discrepancies, issues or weaknesses had been disclosed to the executives responsible for the Company's securities filings. But despite Brown's knowledge of the increased risks described above, including but not limited to the similar attacks on U.S.

Government Agency A and Cybersecurity Firm B, SolarWinds repeatedly failed to disclose the known cybersecurity risks in the Company's periodic reports, rendering them materially misleading.

299. Instead, in quarterly reports on Forms 10-Q from the first quarter of 2020 through the third quarter of 2020, filed on May 8, 2020, August 10, 2020, and November 5, 2020, SolarWinds stated that there had been "no…material changes" to the risk factors quoted above. Those statements were materially false and misleading. A reasonable investor, considering whether to purchase or sell SolarWinds stock, would have considered it important to know the true risks facing the Company (including both the ongoing cybersecurity controls and the increased risks to Orion), not merely generic risk disclosures. This is especially the case because Orion represented 45% of SolarWinds' revenue in the first nine months of 2020 and there were multiple red flags suggesting both intrusions at SolarWinds and specific problems with Orion. The attacks also affected SolarWinds' MSP products, which Brown had likewise described as a "crown jewel."

300. As described above, SolarWinds and Brown knew, or were reckless or negligent in not knowing, that the risk disclosure in the listed SEC filings contained materially false and misleading statements, and that SolarWinds omitted and failed to disclose (either in the SEC filings or elsewhere) the true state of SolarWinds' cybersecurity risks, including the issues, attacks, and violations discussed above. Those omissions made the statements made, in light of the circumstances, misleading.

301. Brown signed sub-certifications for each quarter during the Relevant Period in which he certified in relevant part that:

> The processes listed below as part of the designed internal controls over financial reporting are adequately designed, documented, and the associated key controls

> have been adequately performed to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for internal and bank reporting purposes in accordance with generally accepted accounting principles. All discrepancies, issues or weaknesses have been communicated to the CFO and/or President.
>
> …I have reviewed the represented control matrix for the quarter stated above to ensure to the best of my knowledge that the controls accurately reflects [sic] the procedures performed (all material changes to the process have been properly documented) and in my opinion all of the key controls have been identified.

302. In documents attached to, or referred to by, these certifications, Brown is designated as responsible for certifying these issues for the Information Technology General Computing Controls relating to "Security."

303. As Brown knew, or was reckless or negligent in not knowing, that certification was false because the numerous, documented cybersecurity failures prevented SolarWinds from having effective controls.

304. Additionally and alternatively, the SolarWinds employees involved in and responsible for these issues, including those described above, collectively knew, or were recklessness or negligent in not knowing, that the SEC filings listed above were false for the reasons described above.

F. Once SolarWinds Learned of the SUNBURST Attack, It Did Not Fully Disclose Its Known Impact.

1. In December 2020, a Third SolarWinds Customer Detected Orion Problems and Uncovered the SUNBURST Attack.

305. In December 2020, yet another SolarWinds customer, Cybersecurity Firm C, notified SolarWinds of an attack against its Orion platform. After identifying the attack and determining that the Orion platform was the likely attack vector, Cybersecurity Firm C reverse-engineered the SolarWinds' code to identify what was causing the malicious activity. Within a matter of days, Cybersecurity Firm C had identified the root cause of the malicious activity

within the Orion software code, something SolarWinds itself had been unable to do at any point since the May 2020 U.S. Government Agency A attack.

306. Cybersecurity Firm C contacted SolarWinds' CEO on December 12, 2020, and explained that there was a vulnerability in the Orion software as a result of malicious code that had been inserted into the Orion product by a threat actor. Cybersecurity Firm C shared the decompiled code with SolarWinds during a call with Brown and others on December 12, 2020.

307. Upon reviewing the decompiled code, and no later than December 13, 2020, Brown immediately linked the Cybersecurity Firm C attack to both the earlier May 2020 attack against U.S. Government Agency A and the October 2020 attack against Cybersecurity Firm B. According to Brown's sworn testimony, there was no additional work that he or SolarWinds needed to do to link the May and October 2020 attacks to the malicious code provided by Cybersecurity Firm C in December:

> Q: …Was there additional analysis that was done to determine that happened in the [Cybersecurity Firm B] incident and it happened in the [U.S. Government Agency A] incident?
>
> A: It wasn't necessary, right? The code that he saw that was dropped that was supplied by [Cybersecurity Firm C], decompiled code gave us a full path. And there is plenty of investigation to show that, okay, business layer host was involved. This was a stream of data -- this is what -- oh, this matched what [U.S. Government Agency A] had seen. So it wasn't trying to attack us, it had a different purpose. So it became very, very apparent extremely quickly that that's what the cases were.

2. SolarWinds Made Materially False and Misleading Public Statements About the SUNBURST Attack.

308. After learning on December 12, 2020, that malicious code had been inserted into the Orion platform, Brown and other executives worked to prepare a Form 8-K announcing the vulnerability. Brown participated in drafting the Form 8-K and was responsible for confirming the accuracy of the technical statements made in it.

309. On December 14, 2020, SolarWinds filed a Form 8-K with the SEC that publicly disclosed the SUNBURST attack but created a materially misleading picture of the Company's knowledge of the impact of the attack in at least three respects.

310. First, the December 14, 2020 Form 8-K stated that SolarWinds had "been made aware of a cyberattack that inserted a vulnerability[12] within its Orion monitoring products which, if present and activated, ***could potentially allow*** an attacker to compromise the server on which the Orion products run." SolarWinds knew that this vulnerability was not theoretical but rather, as described above, that the vulnerability when downloaded, installed, and connected to the internet definitively allowed the attacker to compromise the server on which the Orion products were running. In fact, SolarWinds knew that attackers had already utilized the vulnerability to do so on at least three occasions (U.S. Government Agency A, Cybersecurity Firm B, and Cybersecurity Firm C) since at least May 2020.

311. Second, SolarWinds stated that it hired third-party cybersecurity experts to assist in an investigation of these matters, including "***whether a vulnerability in the Orion monitoring products was exploited*** as a point of any infiltration of any customer systems." In fact, SolarWinds knew that the vulnerability had been exploited as a point of infiltration of customers' systems on at least three prior occasions—in the U.S. Government Agency A, Cybersecurity Firm B, and Cybersecurity Firm C incidents.

312. Third, SolarWinds stated that it was "***still investigating whether, and to what extent, a vulnerability in the Orion products was successfully exploited***" in any reported attacks. In fact, SolarWinds knew the vulnerability in the Orion products had been successfully

[12] It would have been more accurate for SolarWinds to say that malicious code had been inserted rather than that a vulnerability had been inserted.

exploited on at least three prior occasions (U.S. Government Agency A, Cybersecurity Firm B, and Cybersecurity Firm C) since as early as May 2020.

313. These misstatements were material because to cybersecurity professionals, users of SolarWinds products, and SolarWinds investors there is a difference in the risk posed by a vulnerability that could potentially be exploited, and one that actually has been exploited on multiple occasions over a six month period. What made the three disclosures above misleading was not that they said that SolarWinds still had more investigating to do (which was true), but that the statements obscured what SolarWinds already knew: (1) the SUNBURST code was not just something that "could ***potentially*** allow an attacker to compromise" a server—rather, it had actually done so on multiple occasions over six months, (2) there was not an open question regarding "***whether*** a vulnerability in the Orion monitoring products was exploited as a point of any infiltration of any customer systems"—rather, it had already been used against U.S. Government Agency A to send information about the server it was located on to threat actors and used at Cybersecurity Firm B to download malicious code; and (3) it was not unknown "***whether***…a vulnerability in the Orion products was successfully exploited" as it clearly had been at least U.S. Government Agency A, which Brown and his InfoSec team described in a July 10, 2020 presentation as a "customer compromise" and "attack that was successful."

314. Brown—who, among other things, was an officer of SolarWinds, head of its InfoSec group, and its point person on cybersecurity issues—participated in the meeting when this statement was drafted, assisted in drafting it, and was responsible for reviewing it and approving its technical/factual accuracy. When the statement was drafted, Brown knew, or was reckless or negligent in not knowing, that the attacks against Cybersecurity Firm C and those against U.S. Government Agency A and Cybersecurity Firm B, were connected. And Brown

therefore knew, or was reckless or negligent in not knowing, that the Form 8-K contained materially false and misleading statements, and that during the Relevant Period SolarWinds omitted and failed to disclose (either in the Form 8-K filings or elsewhere) the true impact of SUNBURST, including the connections to the attacks on U.S. Government Agency A, Cybersecurity Firm B, and Cybersecurity Firm C discussed above. Those omissions made the statements made, in light of the circumstances, misleading. Additionally, while being tasked with the technical accuracy of the Form 8-K, Brown failed to ensure that it was accurate, and failed to ensure that the other persons involved in drafting it had sufficient information to draft it accurately.

315. Even if the way Orion acted at U.S. Government Agency A and Cybersecurity Firm B is not considered an "infiltration" as SolarWinds used that term in the Form 8-K, it was still misleading by omission to fail to disclose those incidents, when SolarWinds (1) had previously concluded that the U.S. Government Agency A attack was a "customer compromise" and an "attack that was successful" and (2) knew that the Cybersecurity Firm B attack was a "breach" that involved the actual download of malicious files onto the customer's Orion server. Omitting any information about these incidents failed to present the true risk the attack posed. There is a material difference between a vulnerability that could be exploited, and malicious files which actively misbehaved by reaching out to apparently malicious websites to provide information or download additional malicious files. Additionally, because the U.S. Government Agency A attack had taken place in May, the failure to disclose these incidents in the December 14, 2020 8-K obscured the length of time the threat actors had been actively using SUNBURST to attack SolarWinds customers, another material fact.

316. Brown's knowledge, recklessness, and/or negligence is attributable to the Company by virtue of his role in the Company as an officer of SolarWinds, head of its InfoSec group, and chief internal cybersecurity expert, and his presence and involvement in the drafting of the Form 8-K, and his approval of the statement regarding its accuracy.

317. Additionally and alternatively, the SolarWinds employees involved in and responsible for these issues, including those described above, collectively knew, or were reckless or negligent in not knowing, that the Form 8-K was false for the reasons described above.

318. The impact of SolarWinds' December 14, 2020 Form 8-K disclosing the SUNBURST attack resonated with investors, even in its materially misstated form, and SolarWinds' stock price declined more than 16% the day of the announcement and at least another 8% the next day. As the Company provided more information regarding the attacks and the impact on its customers, and as news articles described SolarWinds' preexisting cybersecurity problems, SolarWinds' stock price dropped approximately 35% below its pre-disclosure price by the end of the month.

319. In a Form 8-K filed with the SEC on January 12, 2021, SolarWinds disclosed additional information regarding the SUNBURST attack, including that "we have identified two previous customer support incidents that, with the benefit of hindsight, we believe may be related to SUNBURST," and contained some additional information about the U.S. Government Agency A and Cybersecurity Firm B attacks discussed above, including the months in which they occurred. This information was known to Brown at the time of the December 14, 2020 Form 8-K, but he did not disclose it to anyone else involved in preparing the Form 8-K. The failure to include this information in the December 14, 2020 Form 8-K was not the product of a deliberate decision that doing so would harm any ongoing law enforcement efforts, but was due to Brown's

knowing, reckless, or negligent decision to withhold the material information, that—as discussed above—he had definitively linked the three attacks by December 14, 2020.

G. SolarWinds Had Multiple Internal Controls Failures.

1. SolarWinds Lacked Sufficient Internal Accounting Controls to Protect Its Key Assets.

a. SolarWinds Was Required to Have Reasonable Internal Accounting Controls.

320. As an Exchange Act Section 13(a) reporting company, SolarWinds was required to "devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that…access to assets is permitted only in accordance with management's general or specific authorization." In that regard, SolarWinds was required to develop reasonable safeguards against unauthorized access to Company assets by designing and maintaining reasonable controls to prevent and detect unauthorized access to, or use of, its assets.

321. The cybersecurity controls at issue here were "internal accounting controls" in that they were plans, procedures, and records of SolarWinds concerned with the safeguarding of corporate assets. Cybersecurity policies must be designed and implemented to provide shareholders with reasonable assurances that access to corporate assets – including technology assets, computer code and software for distribution to customers – are limited to authorized users, and thus support the twin goals of corporate accountability and management stewardship over corporate assets underlying Rule 13(b)(2)(B).

322. SolarWinds' information technology network environment, source code, and products were among the Company's most critical assets. As discussed above, Orion was among SolarWinds' "crown jewel" assets. SolarWinds' Code of Conduct also described the Company's software code and information technology infrastructure among its most important assets and emphasized employees' responsibility to protect such information. In its October 18, 2018 Form

S-1, SolarWinds stressed the importance of its "technology infrastructure to sell [its] products and operate [its] business" as well as its customers' reliance on SolarWinds' technology to manage their own information technology infrastructure.

323. SolarWinds assessed the effectiveness of its internal controls using the framework in *Internal Control – Integrated Framework* issued in 2013 by the Committee of Sponsoring Organization of the Treadway Commission ("COSO Framework"). For cybersecurity controls, the COSO Framework requires an organization to select and develop internal control activities over technology that are designed and implemented to restrict technology access rights to authorized users and to protect the entity's assets from external threats. As discussed above, under each of the various assessments SolarWinds used during the Relevant Period, the result was the same: SolarWinds' cybersecurity controls, and specifically its access controls to guard its assets, were deficient.

b. SolarWinds Did Not Have Sufficient Controls to Reasonably Protect Its Critical Assets.

324. As a result of the extensive shortcomings to SolarWinds' cybersecurity controls detailed above, the Company failed to devise and maintain a system of internal controls sufficient to provide reasonable assurance that access to the Company's assets was only in accordance with management's general or specific authorization.

325. SolarWinds did not follow its own certification control concerning cybersecurity, including failing to use and document a list of controls in connection with certifications by Company officials. Brown certified to the effectiveness of the Company's information technology controls around financial reporting. But neither he nor the Company were able to identify the list of relevant controls to the SEC during the SEC's investigation. Brown instead

certified based on his general sense of the quality of those controls, while failing to identify the Company's extensive shortcomings in areas such as access controls.

326. SolarWinds' cybersecurity-related policies and procedures went largely unimplemented or were subject to extensive problems or violations. Numerous internal assessments discussed above showed that during the Relevant Period, the Company had significant lapses around access controls, frequently violated its own internal password policy, and failed to apply SDL to at least some of its products, including the Orion Improvement Program portion of the Orion platform.

2. SolarWinds Had Deficient Disclosure Controls.

327. SolarWinds was also required by Exchange Act Rule 13a-15(a) to maintain disclosure controls and procedures, including controls and procedures designed to ensure that information required to be disclosed by an issuer is accumulated and communicated to management to allow for timely decisions regarding disclosure.

328. SolarWinds failed to maintain controls ensuring that information regarding potentially material cybersecurity risks, incidents, and vulnerabilities was reported to the executives responsible for disclosures. SolarWinds' Incident Response Plan, which Brown was supposed to help implement and maintain, was a critical element of the Company's disclosure controls relating to cybersecurity risks and incidents. Among other things, the Incident Response Plan provided that a report of a product security incident affecting multiple customers or affecting one customer but "for which other customers are susceptible" should be classified as a level 2 / moderate issue and elevated to the CEO, CTO and others. Brown recognized at the time of the attack on U.S. Government Agency A that one possibility was that it was part of an effort to use Orion in a larger attack against customers, yet he did not score the issue as a 2 or report the information the CEO. Several months later, after Brown and others recognized that

Cybersecurity Firm B attack was linked to the U.S. Government Agency A attack, the attacks were still not reported to the CEO, nor was the CTO told about the Cybersecurity Firm B attack. And in December 2020, when Brown had linked both of those attacks to the Cybersecurity Firm C attack, he still did disclose that link to the CEO or anyone else involved in drafting the December 14, 2020 Form 8-K.

329. As described above, Brown signed sub-certifications relied on by the senior executives responsible for signing and certifying the filings that contained the disclosures, confirming that all discrepancies, issues or weaknesses had been disclosed to the executives responsible for the Company's securities filings. Yet Brown failed to sufficiently elevate, and SolarWinds failed to implement and maintain policies to ensure Brown elevated, many of the critical issues discussed above, including the VPN vulnerability.

330. Maintaining appropriate disclosure controls requires more than having written policies. It requires programs, procedures, and a culture of compliance reasonably calculated to ensure that those policies are followed. In this case, the fact that the SolarWinds' executive primarily responsible for cybersecurity at the Company was unaware of the requirements in the Incident Response Plan, or failed to recognize the applicability of the Incident Response Plan notification requirement to a vulnerability in its flagship Orion product, which was sent to thousands of SolarWinds' customers, indicates a lack of adequate programs, procedures or culture reasonably calculated to ensure that known cybersecurity risks and incidents were properly accumulated and communicated to the executives responsible for the Company's public securities disclosures.

331. Alternatively, if SolarWinds did maintain effective disclosure controls, and Brown knowingly, recklessly, or negligently failed to follow those controls, that is relevant evidence of

his overall scienter or negligence regarding the scheme and misstatement allegations discussed above.

FIRST CLAIM FOR RELIEF
Violations of Section 17(a) of the Securities Act
(*Against SolarWinds and Brown*)

332. All of the foregoing paragraphs are incorporated by reference herein.

333. Defendants SolarWinds and Brown, by engaging in the conduct above, singly or in concert with others, in the offer or sale of securities, by the use of means or instruments of transportation or communication in interstate commerce or by use of the mails, directly or indirectly:

(a) while acting knowingly or recklessly, employed devices, schemes, or artifices to defraud;

(b) while acting knowingly, recklessly, or negligently, obtained money or property by means of untrue statements of a material fact or by omitting to state a material fact necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading; and

(c) while acting knowingly, recklessly, or negligently, engaged in transactions, practices, or courses of business which operated or would operate as a fraud or deceit upon the purchasers of SolarWinds stock.

334. By engaging in the foregoing conduct, Defendants SolarWinds and Brown violated, and unless restrained and enjoined will continue to violate, Section 17(a) of the Securities Act [15 U.S.C. § 77q(a)].

SECOND CLAIM FOR RELIEF
Aiding and Abetting Violations of Section 17(a) of the Securities Act
(Against Brown)

335. All of the foregoing paragraphs are incorporated by reference herein.

336. As alleged above, Defendant SolarWinds violated Section 17(a) of the Securities Act [15 U.S.C. § 77q(a)].

337. Through his false statements, false sub-certifications, and other means alleged above, Defendant Brown knowingly provided substantial assistance to, and thereby aided and abetted, SolarWinds' violations of the securities laws.

338. By engaging in the foregoing conduct, pursuant to Securities Act Section 15(b) [15 U.S.C. § 77o], Defendant Brown violated Securities Act Section 17(a) [15 U.S.C. § 77q(a)].

THIRD CLAIM FOR RELIEF
Violations of Section 10(b) of the Exchange Act and Rule 10b-5(b) Thereunder
(*Against SolarWinds and Brown*)

339. All of the foregoing paragraphs are incorporated by reference herein.

340. By engaging in the conduct described above, Defendants SolarWinds and Brown directly or indirectly, singly or in concert with others, in connection with the purchase or sale of a security and by the use of means or instrumentalities of interstate commerce, or the mails, or of the facilities of a national securities exchange, with scienter:

(a) employed devices, schemes, or artifices to defraud;

(b) made one or more untrue statements of a material fact or omitted to state one or more material facts necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading; and

(c) engaged in acts, practices or courses of business which operated or would operate as a fraud or deceit upon the purchasers of SolarWinds stock, and other persons.

341. By engaging in the foregoing conduct, Defendants SolarWinds and Brown violated, and unless restrained and enjoined will continue to violate, Section 10(b) of the Exchange Act [15 U.S.C. § 78j(b)] and Rule 10b-5 thereunder [17 C.F.R. § 240.10b-5].

FOURTH CLAIM FOR RELIEF
Aiding and Abetting Violations of Exchange Act 10(b) and Rule 10b-5 Thereunder
(Against Brown)

342. All of the foregoing paragraphs are incorporated by reference herein.

343. As alleged above, Defendant SolarWinds violated Exchange Act Section 10(b) [15 U.S.C. § 78j(b)] and Rule 10b-5 thereunder [17 C.F.R. § 240.10b-5].

344. Through his false statements, false sub-certifications, and other means alleged above, Defendant Brown knowingly provided substantial assistance to, and thereby aided and abetted, SolarWinds' violations of the securities laws.

345. By engaging in the foregoing conduct, pursuant to Exchange Act Section 20(e) [15 U.S.C. § 78t(e)], Defendant Brown violated Exchange Act Section 10(b) [15 U.S.C. § 78j(b)] and Rule 10b-5 thereunder [17 C.F.R. § 240.10b-5].

FIFTH CLAIM FOR RELIEF
Violations of Section 13(a) of the Exchange Act
and Exchange Act Rules 12b-20 and 13a-1, 13a-11, and 13a-13 Thereunder
(*Against SolarWinds*)

346. All of the foregoing paragraphs are incorporated by reference herein.

347. Section 13(a) of the Exchange Act [15 U.S.C. § 78m(a)] and Rules 13a-1, 13a-11, and 13a-13 thereunder [17 C.F.R. §§ 240.13a-1, 240.13a-11, and 240.13a-13] require issuers of

registered securities to file with the SEC factually accurate annual reports (on Form 10-K), quarterly reports (on Form 10-Q), and current reports (on Form 8-K). Exchange Act Rule 12b-20 [17 C.F.R. § 240.12b-20] provides that, in addition to the information expressly required to be included in a statement or report, there shall be added such further material information, if any, as may be necessary to make the required statements, in light of the circumstances under which they were made, not misleading.

348. By engaging in the foregoing conduct, Defendant SolarWinds violated Section 13(a) of the Exchange Act [15 U.S.C. § 78m(a)] and Rules 12b-20, 13a-1, 13a-11, and 13a-13 thereunder [17 C.F.R. §§ 240.12b-20, 240.13a-1, 240.13a-11, and 240.13a-13].

SIXTH CLAIM FOR RELIEF
Aiding and Abetting Violations of Exchange Act Section 13(a) and Rules 12b-20, 13a-1, 13a-11, and 13a-13
(Against Brown)

349. All of the foregoing paragraphs are incorporated by reference herein.

350. As alleged above, Defendant SolarWinds violated Exchange Act Section 13(a) and Rules 12b-20, 13a-1, 13a-11, and 13a-13.

351. Through his false statements, false sub-certifications, and other means alleged above, Defendant Brown knowingly provided substantial assistance to, and thereby aided and abetted, SolarWinds' violations of the securities laws.

352. By engaging in the foregoing conduct, pursuant to Exchange Act Section 20(e) [15 U.S.C. § 78t], Defendant Brown violated Exchange Act Section 13(a) [15 U.S.C. § 78m(a)] and Rules 12b-20, 13a-1, 13a-11, and 13a-13 [17 C.F.R. §§ 240.12b-20, 240.13a-1, 240.13a-11, and 240.13a-13].

SEVENTH CLAIM FOR RELIEF
Violations of Section 13(b)(2)(B) of the Exchange Act
(*Against SolarWinds*)

353. All of the foregoing paragraphs are incorporated by reference herein.

354. By engaging in the conduct described above, SolarWinds failed to devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that access to SolarWinds' assets is permitted only in accordance with management's general or specific authorization, in violation of Exchange Act Section 13(b)(2)(B) [15 U.S.C. § 78m(b)(2)(B)].

355. By reason of the foregoing, SolarWinds violated Exchange Act Section 13(b)(2)(B) [15 U.S.C. § 78m(b)(2)(B)].

EIGHTH CLAIM FOR RELIEF
Aiding and Abetting Violations of 13(b)(2)(B) of the Exchange Act
(*Against Brown*)

356. All of the foregoing paragraphs are incorporated by reference herein.

357. As alleged above, Defendant SolarWinds violated Exchange Act Section 13(b)(2)(B) [15 U.S.C. § 78m(b)(2)(B)].

358. Through his false sub-certifications attesting to the adequacy of SolarWinds' cybersecurity internal controls and other means alleged above, Defendant Brown knowingly provided substantial assistance to, and thereby aided and abetted, SolarWinds' violations of the securities laws.

359. By engaging in the foregoing conduct, pursuant to Exchange Act Section 20(e) [15 U.S.C. § 78t(e)], Defendant Brown violated Section 13(b)(2)(B) of the Exchange Act [15 U.S.C. § 78m(b)(2)(B)].

NINTH CLAIM FOR RELIEF
Violations of Exchange Act Rule 13a-15(a)
(Against SolarWinds)

360. All of the foregoing paragraphs are incorporated by reference herein.

361. Exchange Act Rule 13a-15(a) requires publicly traded companies to maintain disclosure controls and procedures that, as defined in Rule 13a-15(e), "are designed to ensure that information required to be disclosed by the issuer" in reports it files with the SEC "is recorded, processed, summarized and reported" in a timely fashion. And that "[d]isclosure controls and procedures include, without limitation, controls and procedures designed to ensure that information required to be disclosed by an issuer in the reports that it files or submits under the Act is accumulated and communicated to the issuer's management, including its principal executive and principal financial officers, or persons performing similar functions, as appropriate to allow timely decisions regarding required disclosure." Exchange Act Rule 13a-15(e) [17 C.F.R. § 240.13a-15(e)].

362. By engaging in the foregoing conduct, Defendant SolarWinds violated Exchange Act Rule 13a-15(a) [17 C.F.R. § 240.13a-15(a)].

TENTH CLAIM FOR RELIEF
Aiding and Abetting Violations of Exchange Act Rule 13a-15(a)
(Against Brown)

363. All of the foregoing paragraphs are incorporated by reference herein.

364. As alleged above, Defendant SolarWinds violated Exchange Act Rule 13a-15(a) [17 C.F.R. § 240.13a-15(a)].

365. Through his false statements, false sub-certifications, failure to elevate or disclose the VPN, U.S. Government Agency A, or Cybersecurity Firm B incidents, and other means alleged above, Defendant Brown knowingly provided substantial assistance to, and thereby aided and abetted, SolarWinds' violations of the securities laws.

366. By engaging in the foregoing conduct, pursuant to Exchange Act Section 20(e) [15 U.S.C. § 78t], Defendant Brown violated Exchange Act Rule 13a-15(a) [17 C.F.R. § 240.13a-15(a)].

PRAYER FOR RELIEF

WHEREFORE, the SEC respectfully requests that this Court enter a Final Judgment:

A. Finding that Defendants SolarWinds and Brown committed the violations alleged in this Amended Complaint;

B. Permanently restraining and enjoining Defendants SolarWinds and Brown from violating, directly or indirectly, Section 17(a) of the Securities Act [15 U.S.C. § 77q(a)], Sections 10(b), 13(a) and 13(b)(2)(B) of the Exchange Act [15 U.S.C. §§ 78j(b), 78m(a), 78m(b)(2)(B)], and Rules 10b-5, 12b-20, 13a-1, 13a-11, 13a-13, and 13a-15(a) thereunder [17 C.F.R. §§ 240.10b-5, 240.12b-20, 240.13a-1, 240.13a-11, 240.13a-13, and 240.13a-15(a)];

C. Ordering Defendants SolarWinds and Brown to disgorge all ill-gotten gains they received directly or indirectly as a result of the alleged violations, with pre-judgment interest thereon, pursuant to Exchange Act Sections 21(d)(3), (5), and (7) [15 U.S.C. §§ 78u(d)(3), (5) and (7)];

D. Ordering Defendants SolarWinds and Brown to pay civil monetary penalties pursuant to Section 20(d) of the Securities Act [15 U.S.C. § 77t(d)], and Section 21(d)(3) of the Exchange Act [15 U.S.C. § 78u(d)(3)];

E. Permanently prohibiting Defendant Brown, under Section 20(e) of the Securities Act [15 U.S.C. § 77t(e)] and Section 21(d)(2) of the Exchange Act [15 U.S.C. § 78u(d)(2)], from acting as an officer or director of any issuer that has a class of securities registered under Section

12 of the Exchange Act [15 U.S.C. § 78l] or that is required to file reports under Section 15(d) of the Exchange Act [15 U.S.C. § 78o(d)]; and

F. Granting any other and further relief this Court may deem just and proper.

JURY DEMAND

Pursuant to Federal Rule of Civil Procedure 38, the SEC demands a trial by jury on all issues so triable.

Dated: February 16, 2024

Respectfully submitted,

/s/ Christopher M. Bruckmann
Christopher M. Bruckmann
(SDNY Bar No. CB-7317)
Kristen M. Warden
(admitted *pro hac vice*)
John J. Todor
(admitted *pro hac vice*)
William B. Ney
(admitted *pro hac vice*)
Benjamin Brutlag
(SDNY Bar No. BB-1196)
Lory Stone
(admitted *pro hac vice*)
Securities and Exchange Commission
100 F Street, NE
Washington, D.C. 20549
202-551-5986 (Bruckmann)
202-551-4661 (Warden)
202-551-5317 (Ney)
202-551-2421 (Brutlag)
202-551-4931 (Stone)
202-551-5381 (Todor)
BruckmannC@sec.gov
WardenK@sec.gov
TodorJ@sec.gov
NeyW@sec.gov
BrutlagB@sec.gov
StoneL@sec.gov

Attorneys for Plaintiff Securities and Exchange Commission